UNIVERSIDAD MAYOR DE SAN ANDRES
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
CARRERA DE DERECHO

T E S I S D E G R A D O

SEGURIDAD JURÍDICA DE LOS DOCUMENTOS ELECTRÓNICOS

TESIS DE GRADO PRESENTADO PARA OPTAR EL GRADO DE LICENCIADA EN DERECHO

POSTULANTE: MASIEL ANGELA DIAZ MIRANDA
TUTOR: DR. MARCELO FERNÁNDEZ IRAOLA

LA PAZ – BOLIVIA
2006

AGRADECIMIENTOS

A mis padres por su apoyo,
comprensión, fe y confianza.

Asimismo, al Dr. Marcelo Fernández
Iraola, por su valiosa orientación y guía
en la elaboración de este trabajo

A mi hijita Rubi Antonella

ÍNDICE

INTRODUCCIÓN

El grado de inseguridad en la actual sociedad es extremo y se manifiesta en todos los ámbitos de la misma. Por tanto, es engañoso todo intento de fingir una seguridad que no existe y más aún, en esta época de avances tecnológicos, en que la informática, la cibernética, la computación y los sistemas informáticos no son ajenos a la inseguridad.

El uso de cajeros automáticos, las compras por Internet, el navegar por la red, la contratación por Internet, el Chat, la pornografía infantil en línea, la piratería de programas, la piratería de la información (consistente en acceder a bases de datos sin autorización, actividad comúnmente conocida como hacker o piratas cibernéticos), los fraudes bancarios, los derechos de autor sobre material publicado en Internet, las declaraciones fiscales, el uso de tarjetas de crédito en terminales, las declaraciones patrimoniales de los servidores públicos, los casinos en red, el correo electrónico, y la contaminación y destrucción de información que se encuentra en equipos de cómputo (mediante el envío de virus), son algunos ejemplos de inseguridad informática, que por los nuevos tipos de documentos que se presentan, avanzan hacia la denominada inseguridad de documentos electrónicos.

El mundo avanza de forma acelerada en todo cuanto tiene que ver con el desarrollo de tecnologías de información y comunicaciones, surgiendo nuevas formas de trabajar, aprender, comunicarse y celebrar negocios; borrando fronteras y acortando distancias.

El gran desarrollo tecnológico y su aplicación directa en la vida diaria, ha revolucionado los patrones de comportamiento humano y por ende las relaciones sociales entre los hombres, de las cuales surgen también las nuevas relaciones jurídicas de carácter informático.

En el mundo de la informática puede palparse un sentimiento de inseguridad, por falta de regulación específica y de un control efectivo respecto de todas las actividades que inciden en la materia. El común de la gente puede ver dispersión y desconocimiento del marco jurídico que debe aplicarse a la informática, originándose temor y desconfianza. Durante la última década los incidentes de inseguridad han crecido de manera alarmante estableciendo un escenario oscuro sobre la seguridad de las infraestructuras de computación en el mundo.

En los sistemas informáticos, existe inseguridad jurídica, y en esos sistemas informáticos se guardan documentos diversos. Por lo tanto, un documento electrónico esta expuesto a la manipulación, alteración, destrucción y falsificación. Sobre todo cuando nos conectamos a Internet, que esta integrada por un vasto conjunto de máquinas que conforman una enorme red fuertemente interconectada y donde es posible leer el contenido de los paquetes, destruirlos e, incluso,

modificarlos, posibilitando todo tipo de ataques contra la confidencialidad autenticidad y la integridad de los documentos electrónicos.

Debido a que el Internet es un sistema global de información, el efecto de aldea global generado por el entramado de redes y la proliferación de nodos en todo el planeta ayudan a la difusión inmediata de los mensajes y permite el acceso a cualquier información introducida en la red,. A las reconocidas ventajas que ello supone se unen las distorsiones y los malos usos que pueden tener lugar en el sistema y que confirman una vez más la falta de protección y la inseguridad jurídica en los documentos electrónicos.

Por este motivo, debe existir un marco jurídico de protección. Un marco jurídico que regule de forma prioritaria y fundamental el documento electrónico como medio probatorio, como instrumento base de validación de los derechos de las personas, así como en el comercio o los contratos electrónicos se debería tener en cuenta algunos pasos técnicos que deben darse para celebrar un contrato y tender hacia la consecución de un marco jurídico adecuado, donde existan mecanismos o políticas, que brinde seguridad jurídica en esta importante faceta de la vida moderna.

La tendencia internacional es recoger en su normativa a los documentos electrónicos seguros para permitir un desarrollo uniforme en los mercados. De existir incompatibilidades tecnológicas los mercados no se podrían integrar, es por ello que se hace necesario establecer reglas claras, así como medidas que

procuren la efectividad, protección y seguridad del documento electrónico. Sin embargo en el contexto internacional, son pocos los países que cuentan con una legislación apropiada, por eso es necesaria una regulación global, una normativa uniforme, mediante el establecimiento de una política común con un marco institucional apropiado y eficaz para la concertación y el desarrollo, junto con el mejoramiento de los sistemas informáticos de control y seguridad con el fin de inducir a la confianza a las personas e instituciones en sus actos y relaciones jurídicas.

Esta temática planteada sobre la seguridad e inseguridad de los documentos electrónicos, es abordada en la presente tesis, analizando los factores esenciales del problema, arribando a las conclusiones más importantes y planteando mínimas recomendaciones que nos permitan superar las dificultades e insuficiencias legales de la información de los medios e instrumentos informáticos en nuestra sociedad.

CAPITULO I

IMPORTANCIA DE LA COMPUTACIÓN

Los acelerados avances científicos y el gran impacto tecnológico han llegado a afectar a todos los sectores y áreas de la sociedad, como por ejemplo; en las comunicaciones, en la medicina, en la educación, en el ámbito de la información, y por supuesto también en el mundo jurídico. Las computadoras se han convertido en la actualidad en la principal herramienta utilizada por el hombre y ya son parte esencial e inseparable de cada uno de nosotros.

Por siglos los hombres han tratado de usar fuerzas y artefactos de diferente tipo para realizar sus trabajos, para hacerlos más simples y rápidos, para solucionar sus múltiples problemas y hacer su vida mas efectiva y practica. Así ha producido maquinas que facilitan los cálculos y operaciones de procesamiento de información diversa, cuya historia conocida de los artefactos que calculan, se remonta a muchos años antes de Jesucristo.

1.1. HISTORIA DE LA COMPUTACIÓN.[1]*

Uno de los primeros dispositivos mecánicos para contar fue el ábaco, que apareció el 500 A.C. en la cultura babilónica, que servia para agilizar las operaciones aritméticas básicas y que se extendió a China y Japón, siendo descubierto mucho mas tarde por Europa.[2] Este dispositivo es muy sencillo, consta de cuentas ensartadas en varillas que a su vez están montadas en un marco rectangular, al desplazar las cuentas sobre varillas, sus posiciones representan valores almacenados, y es mediante dichas posiciones que este representa y almacena datos. A este dispositivo no se le puede llamar computadora por carecer del elemento fundamental llamado programa.

Otro de los inventos mecánicos fue la Pascalina inventada por Blaise Pascal (1623 - 1662) de Francia y la de Gottfried Wilhelm von Leibniz (1646 - 1716) de Alemania. Con estas máquinas, los datos se representaban mediante las posiciones de los engranajes, y los datos se introducían manualmente estableciendo dichas posiciones finales de las ruedas, de manera similar a como leemos los números en el cuentakilómetros de un automóvil.

---

[1] * La historia de la computación que se detalla en este capitulo es un extracto de diversas paginas Web, similares en su mayoría y que se las cita por ética de referencia en forma global.

[2] www.monografias.com/trabajos/histocomp/histocomp.shtml

La primera computadora fue la maquina analítica creada por Charles Babbage, profesor matemático de la Universidad de Cambridge en el siglo XIX. La idea que tuvo Charles Babbage sobre un computador nació debido a que la elaboración de las tablas matemáticas era un proceso tedioso y propenso a errores. En 1823 el gobierno Británico lo apoyo para crear el proyecto de una máquina de diferencias, un dispositivo mecánico para efectuar sumas repetidas.[3]

Mientras tanto Charles Jacquard (francés), fabricante de tejidos, había creado un telar que podía reproducir automáticamente patrones de tejidos leyendo la información codificada en patrones de agujeros perforados en tarjetas de papel rígido. Al enterarse de este método Babbage abandonó la máquina de diferencias y se dedicó al proyecto de la máquina analítica que se pudiera programar con tarjetas perforadas para efectuar cualquier cálculo con una precisión de 20 dígitos. La tecnología de la época no bastaba para hacer realidad sus ideas. El mundo no estaba listo, y no lo estaría por cien años más.

En 1944 se construyó en la Universidad de Harvard, la Mark I, diseñada por un equipo encabezado por Howard H. Aiken.[4] Esta máquina no está considerada como computadora electrónica debido a que no era de propósito general y su

[3] www.monografias.com/trabajos/histocomp/histocomp.shtml

[4] www.monografias.com/trabajos/histocomp/histocomp.shtml

funcionamiento estaba basado en dispositivos electromecánicos llamados relevadores.

En 1947 se construyó en la Universidad de Pennsylvania la ENIAC (Electronic Numerical Integrator And Calculator) que fue la primera computadora electrónica, el equipo de diseño lo encabezaron los ingenieros John Mauchly y John Eckert.[5] Esta máquina ocupaba todo un sótano de la Universidad, tenía más de 18 000 tubos de vacío, consumía 200 KW de energía eléctrica y requería todo un sistema de aire acondicionado, pero tenía la capacidad de realizar cinco mil operaciones aritméticas en un segundo.

El proyecto, auspiciado por el departamento de Defensa de los Estados Unidos, culminó dos años después, cuando se integró a ese equipo el ingeniero y matemático húngaro John von Neumann (1903 - 1957). Las ideas de von Neumann resultaron tan fundamentales para su desarrollo posterior, que es considerado el padre de las computadoras.

La EDVAC (Electronic Discrete Variable Automatic Computer) fue diseñada por este nuevo equipo. Tenía aproximadamente cuatro mil bulbos y usaba un tipo de

[5] www.monografias.com/trabajos/histocomp/histocomp.shtml

memoria basado en tubos llenos de mercurio por donde circulaban señales eléctricas sujetas a retardos.

La idea fundamental de von Neumann fue: permitir que en la memoria coexistan datos con instrucciones, para que entonces la computadora pueda ser programada en un lenguaje, y no por medio de alambres que eléctricamente interconectaban varias secciones de control, como en la ENIAC.[6] Todo este desarrollo de las computadoras suele divisarse por generaciones.

1.1.1. PRIMERA GENERACIÓN.

En esta generación había un gran desconocimiento de las capacidades de las computadoras, puesto que se realizó un estudio en esta época que determinó que con veinte computadoras se saturaría el mercado de los Estados Unidos en el campo de procesamiento de datos. Esta generación abarco la década de los cincuenta, y se conoce como la primera generación. Estaban construidas por medio de tubos de vacío, eran programadas en lenguaje de máquina.

En esta generación las máquinas son grandes y costosas (de un costo aproximado de cientos de miles de dólares). En 1951 aparece la UNIVAC UNIVersAl Computer), fue la primera computadora comercial, que disponía de mil

[6] PRE-historia de la Computación. La pre-historia de la Era de la Computación. Jorge Machado Lima-Perú.

palabras de memoria central y podían leer cintas magnéticas, se utilizó para procesar el censo de 1950 en los Estados Unidos.[7]

En las dos primeras generaciones, las unidades de entrada utilizaban tarjetas perforadas, retomadas por Herman Hollerith (1860 - 1929), quien además fundó una compañía que con el paso del tiempo se conocería como IBM (International Bussines Machines). Después se desarrolló por IBM la *IBM 701* de la cual se entregaron 18 unidades entre 1953 y 1957. Posteriormente, la compañía Remington Rand fabricó el modelo 1103, que competía con la 701 en el campo científico, por lo que la IBM desarrolló la 702, la cual presentó problemas en memoria, debido a esto no duró en el mercado. La computadora más exitosa de la primera generación fue la IBM 650, de la cual se produjeron varios cientos.[8] Esta computadora que usaba un esquema de memoria secundaria llamado tambor magnético, que es el antecesor de los discos actuales.

Otros modelos de computadora que se pueden situar en los inicios de la segunda generación son: la UNIVAC 80 y 90, las IBM 704 y 709, Burroughs 220 y UNIVAC 1105.

1.1.2. SEGUNDA GENERACIÓN.

---

[7] www.perantivirus.com/historia/

[8] AZPILCUETA, Hermilio. Derecho Informático, Ed. Abeledo- Perrot Buenos aires Argentina, 1987. 18-30.

Cerca de la década de 1960, las computadoras seguían evolucionando, se reducía su tamaño y crecía su capacidad de procesamiento. También en esta época se empezó a definir la forma de comunicarse con las computadoras, que recibía el nombre de programación de sistemas. Están construidas con circuitos de transistores, se programan en nuevos lenguajes llamados lenguajes de alto nivel.

En esta generación las computadoras se reducen de tamaño y son de menor costo. Aparecen muchas compañías y las computadoras eran bastante avanzadas para su época como la serie 5000 de Burroughs y la ATLAS de la Universidad de Manchester. Algunas de estas computadoras se programaban con cintas perforadas y otras más por medio de cableado en un tablero. Los programas eran hechos a la medida por un equipo de expertos: analistas, diseñadores, programadores y operadores que se manejaban como una orquesta para resolver los problemas y cálculos solicitados por la administración.

El usuario final de la información no tenía contacto directo con las computadoras. Esta situación en un principio se produjo en las primeras computadoras personales, pues se requería saberlas "programar" (alimentarle instrucciones) para obtener resultados; por lo tanto su uso estaba limitado a aquellos audaces pioneros que gustaran de pasar un buen número de horas escribiendo instrucciones, "corriendo" el programa resultante y verificando y corrigiendo los errores o bugs que aparecieran. Además, para no perder el "programa" resultante

había que "guardarlo" (almacenarlo) en una grabadora de astte, pues en esa época no había discos flexibles y mucho menos discos duros para la PC; este procedimiento podía tomar de 10 a 45 minutos, según el programa.[9] El panorama se modificó totalmente con la aparición de las computadoras personales con mejore circuitos, más memoria, unidades de disco flexible y sobre todo con la aparición de programas de aplicación general en donde el usuario compra el programa y se pone a trabajar. Aparecen los programas procesadores de palabras como el célebre Word Star, la impresionante hoja de cálculo (spreadsheet) Visicalc y otros más que de la noche a la mañana cambian la imagen de la PC. El software empieza a tratar de alcanzar el paso del hardware. Pero aquí aparece un nuevo elemento: el usuario.

El usuario de las computadoras va cambiando y evolucionando con el tiempo. De estar totalmente desconectado a ellas en las máquinas grandes pasa la PC a ser pieza clave en el diseño tanto del hardware como del software. Aparece el concepto de human interfase que es la relación entre el usuario y su computadora. Se habla entonces de hardware ergonómico (adaptado a las dimensiones humanas para reducir el cansancio), diseños de pantallas antirreflejos y teclados que descansen la muñeca. Con respecto al software se inicia una verdadera

---

[9] ROZAR, Theodore, El culto a la información. El folclore de los ordenadores y el verdadero arte de pensar (Trad. de Jordi Beltrán). México, Consejo Nacional para la Cultura y las Artes, Grijalbo, 1990, 277 p.p.

carrera para encontrar la manera en que el usuario pase menos tiempo capacitándose y entrenándose y más tiempo produciendo. Se ponen al alcance programas con menús (listas de opciones) que orientan en todo momento al usuario (con el consiguiente aburrimiento de los usuarios expertos); otros programas ofrecen toda una artillería de teclas de control y teclas de funciones (atajos) para efectuar toda suerte de efectos en el trabajo (con la consiguiente desorientación de los usuarios novatos). Se ofrecen un sinnúmero de cursos prometiendo que en pocas semanas hacen de cualquier persona un experto en los programas comerciales. Pero el problema "constante" es que ninguna solución para el uso de los programas es "constante". Cada nuevo programa requiere aprender nuevos controles, nuevos trucos, nuevos menús. Se empieza a sentir que la relación usuario-PC no está acorde con los desarrollos del equipo y de la potencia de los programas. Hace falta una relación amistosa entre el usuario y la PC.[10]

Las computadoras de esta generación fueron: la Philco 212 (esta compañía se retiró del mercado en 1964) y la UNIVAC M460, la Control Data Corporation modelo 1604, seguida por la serie 3000, la IBM mejoró la 709 y sacó al mercado la 7090, la National Cash Register empezó a producir máquinas para proceso de datos de tipo comercial, introdujo el modelo NCR 315. La Radio Corporation of

---

[10] MENTOR INTERACTIVO.- Océano.- Enciclopedia temática estudiantil. España.2004.

América introdujo el modelo 501, que manejaba el lenguaje COBOL, para procesos administrativos y comerciales. Después salió al mercado la RCA 601[11].

1.1.3. TERCERA GENERACIÓN.

Con los progresos de la electrónica y los avances de la comunicación con las computadoras en el año de 1960, surge la tercera generación de las computadoras. Se inaugura con la IBM 360 en abril de 1964.3.[12]

Su fabricación electrónica esta basada en circuitos integrados, su manejo es por medio de los lenguajes de control de los sistemas operativos. La IBM produce la serie 360 con los modelos 20, 22, 30, 40, 50, 65, 67, 75, 85, 90, 195 que utilizaban técnicas especiales del procesador, unidades de cinta de nueve canales, paquetes de discos magnéticos y otras características que ahora son estándares (no todos los modelos usaban estas técnicas, sino que estaba dividido por aplicaciones). El sistema operativo de la serie 360, se llamó OS que contaba con varias configuraciones, incluía un conjunto de técnicas de manejo de memoria y del

---

[11] Jurisprudencia Argentina.-Tomo II- Año 1999- "Documento Electrónico" por Daniel Altmark, págs. 851-855.

[12] www.perantivirus.com/historia/

procesador que pronto se convirtieron en estándares. En 1964 CDC introdujo la serie 6000 con la computadora 6600 que se consideró durante algunos años como la más rápida.

En el año de 1970, la IBM produce la serie 370 (modelos 115, 125, 135, 145, 158, 168). UNIVAC compite con los modelos 1108 y 1110, máquinas en gran escala; mientras que CDC produce su serie 7000 con el modelo 7600. Estas computadoras se caracterizan por ser muy potentes y veloces.[13] A finales de esta década la IBM de su serie 370 produce los modelos 3031, 3033, 4341. Burroughs con su serie 6000 produce los modelos 6500 y 6700 de avanzado diseño, que se reemplazaron por su serie 7000. Honey - Well participa con su computadora DPS con varios modelos.

A mediados de la década de 1970, aparecen en el mercado las computadoras de tamaño mediano, o mini computadoras que no son tan costosas como las grandes (llamadas también como mainframes que significa también, gran sistema), pero disponen de gran capacidad de procesamiento. Algunas mini computadoras fueron las siguientes: la PDP - 8 y la PDP - 11 de Digital Equipment Corporation, la VAX (Virtual Address extended) de la misma compañía, los modelos NOVA y ECLIPSE

---

[13] ROSZAK, Theodore, El culto a la información. El folclore de los ordenadores y el verdadero arte de pensar (Trad. de Jordi Beltrán). México, Consejo Nacional para la Cultura y las Artes, Grijalbo, 1990, 277 p.p.

de Data General, la serie 3000 y 9000 de Hewlett - Packard con varios modelos el 36 y el 34, la Wang y Honey - Well -Bull, Siemens de origen alemán, la ICL fabricada en Inglaterra. En la Unión Soviética se utilizó la US (Sistema Unificado, Ryad) que ha pasado por varias generaciones.[14]

1.1.4. CUARTA GENERACIÓN.

Aquí aparecen los microprocesadores, un gran adelanto de la microelectrónica, son circuitos integrados de alta densidad y con una velocidad impresionante. Las microcomputadoras con base en estos circuitos, son extremadamente pequeñas y baratas, por lo que su uso se extiende al mercado industrial. Aquí nacen las computadoras personales que han adquirido proporciones enormes y que han influido en la sociedad en general sobre la llamada revolución informática.[15]

.

En 1976 Steve Wozniak y Steve Jobs inventan la primera microcomputadora de uso masivo y más tarde forman la compañía conocida como la Apple que fue la segunda compañía más grande del mundo, antecedida tan solo por IBM;y es una de las cinco compañías más grandes del mundo.

---

[14] CORREA, Carlos. Derecho Informático Ed. Depalma Buenos Aires. Argentina, 1993. 30-42. 85-96.

[15] www.monografias.com/trabajos/histocomp/histocomp.shtml

En 1981 se vendieron 800 000 computadoras personales, al siguiente subió a 1 400 000. Entre 1984 y 1987 se vendieron alrededor de 60 millones de computadoras personales, por lo que no queda duda que su impacto y penetración han sido enormes.[16] Con el surgimiento de las computadoras personales, el software y los sistemas que con ellas se manejan han tenido un considerable avance, porque han hecho más interactiva la comunicación con el usuario. Surgen otras aplicaciones como los procesadores de palabra, las hojas electrónicas de cálculo, paquetes gráficos, etc. También las industrias del Software de las computadoras personales crece con gran rapidez, Gary Kildall y William Gates se dedicaron durante años a la creación de sistemas operativos y métodos para lograr una utilización sencilla de las microcomputadoras (son los creadores de CP/M y de los productos de Microsoft).

No todo son microcomputadoras, por su puesto, las mini computadoras y los grandes sistemas continúan en desarrollo. De hecho las máquinas pequeñas rebasaban por mucho la capacidad de los grandes sistemas de 10 o 15 años antes, que requerían de instalaciones costosas y especiales, pero sería equivocado suponer que las grandes computadoras han desaparecido; por el contrario, su presencia era ya ineludible en prácticamente todas las esferas de control gubernamental, militar y de la gran industria. Las enormes computadoras

[16] Monografias.com - Datos básicos, historia de la computación

de las series CDC, CRAY, Hitachi o IBM por ejemplo, eran capaces de atender a varios cientos de millones de operaciones por segundo.[17]

1.1.5. QUINTA GENERACIÓN.

En vista de la acelerada marcha de la microelectrónica, la sociedad industrial se ha dado a la tarea de poner también a esa altura el desarrollo del software y los sistemas con que se manejan las computadoras. Surge la competencia internacional por el dominio del mercado de la computación, en la que se perfilan dos líderes que, sin embargo, no han podido alcanzar el nivel que se desea: la capacidad de comunicarse con la computadora en un lenguaje más cotidiano y no a través de códigos o lenguajes de control especializados.

Japón lanzó en 1983 el llamado "programa de la quinta generación de computadoras", con los objetivos explícitos de producir máquinas con innovaciones reales en los criterios mencionados.[18] Y en los Estados Unidos ya está en actividad un programa en desarrollo que persigue objetivos semejantes, que pueden resumirse de la siguiente manera:

---

[17] Jurisprudencia Argentina.-Tomo II- Año 1999- "Documento Electrónico" por Daniel Altmark, págs. 851-855.

[18] www.monografias.com/trabajos/histocomp/histocomp.shtml

Procesamiento en paralelo mediante arquitecturas y diseños especiales y circuitos de gran velocidad, manejo de lenguaje natural y sistemas de inteligencia artificial.[19] El futuro previsible de la computación es muy interesante, y se puede esperar que esta ciencia siga siendo objeto de atención prioritaria de gobiernos y de la sociedad en conjunto.

1.1.6. MODELO DE VON NEUMANN.

Las computadoras digitales actuales se ajustan al modelo propuesto por el matemático John Von Neumann. De acuerdo con el, una característica importante de este modelo es que tanto los datos como los programas, se almacenan en la memoria antes de ser utilizados.[20]

1.1.7. EL IMPERIO DE LOS CABLES.

Debemos mencionar también que el gran avance que se realizo en el ámbito de los cables dio un progreso mayor a la informática, pues los adelantos que se producían otorgaron mayor velocidad a la información dentro y fuera de los computadores.

a. Fibra Óptica.

---

[19] www.alfa-redi.org/documento/default.asp

[20] http://www.monografias.com/trabajos14/documentosinformaticos/documentosinformaticos2.shtml

Los circuitos de fibra óptica son filamentos de vidrio flexibles, del espesor de un pelo, llevan mensajes en forma de haces de luz que realmente pasan a través de ellos de un extremo a otro, donde quiera que el filamento vaya (incluyendo curvas y esquinas) sin interrupción. Las fibras ópticas pueden ahora usarse como los alambres de cobre convencionales, tanto en pequeños ambientes autónomos (tales como sistemas de procesamiento de datos de aviones), como en grandes redes geográficas (como los sistemas de largas líneas urbanas mantenidos por compañías telefónicas).[21]

El concepto de las comunicaciones por ondas luminosas ha sido conocido por muchos años, sin embargo, no fue hasta mediados de los años setenta que se publicaron los resultados del trabajo teórico, estos indicaban que era posible confiar un haz luminoso en una fibra transparente y flexible y proveer así un canal analógico óptico de la señalización por alambres electrónicamente. El problema técnico que había que resolver para el avance de la fibra óptica, residía en las fibras mismas, que absorbían luz que dificultaba el proceso. Para la comunicación práctica, la fibra óptica debe transmitir señales luminosas detectables por muchos kilómetros, el vidrio ordinario tiene un haz luminoso de pocos metros, se han desarrollado nuevos vidrios muy puros, con transparencias mucho mayores que la del vidrio ordinario, estos vidrios empezaron a producirse a principios de los setenta, este gran avance dio ímpetu a la industria de las fibras ópticas, ambos

[21]http://www.monografias.com/trabajos14/documentosinformaticos/documentosinformaticos2.shtml

han de ser miniaturizados para componentes de sistemas fibro-ópticos, lo que ha exigido considerable labor de investigación y desarrollo. Los laceres generan luz "coherente" que ni es fuerte ni concentrada, lo que se debe usar depende de los requisitos técnicos para diseñar el circuito de fibras ópticas.

La mayoría de las fibras ópticas se hacen de arena o sílice, materia prima abundante en comparación con el cobre, con unos kilogramos de vidrio pueden fabricarse aproximadamente 43 kilómetros de fibra óptica. Los dos constituyentes esenciales de las fibras ópticas son el núcleo y el revestimiento, el núcleo es la parte más interna de la fibra y es la que guía la luz, consiste en una o varias hebras delgadas de vidrio o de plástico con diámetro de 50 a 125 micras. El revestimiento es la parte que rodea y protege al núcleo, el conjunto de núcleo y revestimiento está a su vez rodeado por un forro o funda de plástico u otros materiales que lo resguardan contra la humedad, el aplastamiento, los roedores, y otros riesgos del entorno. El despliegue tiene en general tres tipos de trazado fundamentales: ruta carretera, vía ferroviaria o líneas de alta tensión.

b. Microondas.

Medio que se usa para enviar señales que contienen el equivalente de grandes cantidades de líneas, pero a través del espacio.[22] Antes del perfeccionamiento de la fibra óptica era el medio favorito para enviar líneas telefónicas y de televisión de

[22] www.monografias.com/trabajos/histocomp/histocomp.shtml

ciudad a ciudad. Ahora se usa para comunicar los continentes a través de los satélites y, nuevamente se está usando para ampliar las alternativas en comunicaciones urbanas y suburbanas.

1.1.8. PRIMERAS REDES INFORMÁTICAS.

Una red es un conjunto de líneas de cobre, fibras ópticas o señales de microondas que inciden en nodos y esos nodos a su vez a través de otras líneas se comunican hacia otros nodos, de modo que el nodo más simple es mi propia computadora personal y entonces, todas las computadoras, sin importar el tamaño, se pueden comunicar entré si para intercambiar información de todo tipo.

a. Arpanet.

En 1969 surge ARPANET, que es una Agencia de Proyectos de Investigación Avanzada de Defensa, del Departamento de Defensa de EE.UU. Es una red experimental en la cual se probaron las teorías de software en los que está basado Internet en la actualidad. Esta red no existe en la actualidad. Esta red gestionada por DARPA, es el origen de Internet, basado en el intento de conectar esta red (ARPANET) a otras redes mediante enlaces de satélite, radio y cableado. Es una red experimental que apoya a la investigación militar, en concreto sobre la resistencia a fallos parciales.[23]

[23]http://www.monografias.com/trabajos14/documentosinformaticos/documentosinformaticos2.shtml

La filosofía de esta red consiste en que cada uno de los ordenadores que componen la misma sea capaz de comunicarse, como elemento individual, con cualquier otra computadora de la red. ARPANET en principio interconectaba 4 grandes ordenadores en localizaciones secretas de EE.UU. DARPA fue quien diseñó específicamente el protocolo de comunicaciones TCP/IP (Transmission Control Protocol/Internet Protocol), extendido actualmente de forma espectacular. 1983: Se desarrolla el servidor de nombres (DNS), evitando direcciones numéricas (a nivel usuario). Frente al incremento de tráfico, se divide la red en MIL (Militar y restringida) y ARPA (Para el resto de comunicación). Frente al incremento de tráfico, se divide la red en MIL (Militar y restringida) y ARPA. Para el resto de comunicación), la unión de ambas se denomina DARPA Internet. Paralelamente, se desarrollan las redes de área local Ethernet con protocolos de comunicación de ARPANET, permitiendo el entendimiento entre redes. (En 1983 aparecen las primeras estaciones de trabajo para escritorio). [24]

Estas redes pertenecen a Universidades, Centros de Investigación y Firmas Comerciales (Usenet, BITnet, EUNet, DECNet). 1984: La NSF (Fundación Nacional de la Ciencia) intenta hacer uso de ARPANet para facilitar el acceso a

[24]http://www.monografias.com/trabajos14/documentosinformaticos/documentosinformaticos2.shtml

cinco Centros de Proceso de Datos, localizados en las principales universidades americanas. Por razones burocráticas no se pudo utilizar ARPANet.

En 1984 la NSF decide crear su propia red, denominada NSFNet, basada en la tecnología ARPANet, que acabaría convirtiéndose en la auténtica espina dorsal de Internet. El número de hosts rebasa los 1.000. El éxito alcanzado fue tal, que hizo necesaria sucesivas ampliaciones de la capacidad de las líneas troncales. NSFNet, es todavía una de las piezas más importantes dentro de Internet. Debido al corte de las líneas telefónicas, se decidió crear redes regionales. El tráfico en la red se incrementó con el tiempo hasta la saturación de los ordenadores centrales y líneas telefónicas.

En 1987 se realizó un contrato para actualizar y administrar la red, con la compañía Merit Network Inc., en colaboración con IBM Y MCI (Microwave Comunnications Incorporated). Se mejoraron las líneas en un factor de 20, con hosts más poderosos. El "gusano" (worm) de Internet, se transmite por la red, afectando a 6.000 ordenadores de los 60.000 que componían la red. 1989: El número de hosts es de 100.000.[25]

El grupo de mayor autoridad sobre el desarrollo de la red es la Internet Society,

[25]http://www.monografias.com/trabajos14/documentosinformaticos/documentosinformaticos2.shtml

creado en 1990 y formado por miembros voluntarios, cuyo propósito principal es promover el intercambio de información global mediante la tecnología Internet. Desaparece ARPANet.

b. Internet

A lo largo de los años ochenta se produce una gran expansión de la red. En 1985 se presenta el "Protocolo de Transferencia de Ficheros" (FTP), que sigue vigente en la actualidad. A lo largo de esta década se conectan a Internet las primeras redes europeas y también japonesas, con lo que la red ya es de ámbito verdaderamente mundial.

A finales de los ochenta se producen grandes cambios, aparecen los primeros "crackers" y "hackers", aparecen los primeros virus "gusano", la agencia ARPA se retira de la red y sobre todo aparece la World Wide Web (la Telaraña Global).[26] Fue Tim Berners-Lee quien, trabajando en el CERN (Centre Européen de Recherche Nucléaire - Ginebra, Suiza) junto con Rober Cailliau inventó el protocolo de transmisión http y el lenguaje HTML en que se basa la "Web".

En 1993 aparece "Mosaic", el primer navegador. El año 1995 empieza la gran expansión de Internet, desde entonces se han superado todas las expectativas. En este año la WWW se consolida como el primero de los servicios que ofrece la

[26] www.lafactoriaweb.com/articulos/sanroma.htm

red.[27] En esta época se produce la aparición de la Internet comercial, las empresas se instalan en la red y se ofrecen todo tipo de servicios "on line", tiendas, bancos,... todo el mundo se instala en el ciberespacio. Es en esta época también, cuando aparecen los primeros motores de búsqueda, el lenguaje "Java" se incorpora a los navegadores, y se desarrollan otras tecnologías orientadas a convertir a la red en un mundo multimedia lo más atractivo posible.

1.1.9. EL CIBERESPACIO.

El ciberespacio es una alucinación social consensuada. La matriz tiene sus raíces en las primitivas galerías de juego, en los primeros programas gráficos y en la experimentación militar con conexiones craneales, Neuromante.[28]

Una enumeración somera de los problemas éticos del ciberespacio nos ofrece la siguiente lista:

1. La privacía: no tanto la posibilidad (real) de fallos en los sistemas de correo que provoquen mensajes que van a lugares equivocados, sino más bien la intromisión intencional. Esta intromisión puede ser desde la del compañero de trabajo que lee nuestro correo hasta el sistemático intervencionismo estatal.

---

[27] http://www.itlibrary.com/reference/library/1575212684/ewtoc.html

[28] GRÜN, Ernesto, Una visión sistémica y cibernética del Derecho. Buenos Aires, Abeledo-Perrot, 1995, 122 p.p.

2. La identidad: es posible esconder la verdadera identidad a la hora de intervenir en una conversación.

3. El respeto a los derechos ajenos: ante la ausencia de mecanismos verbales o no verbales de poder, muchas veces se abusa de la ausencia de una posición de fuerza para provocar o motivar reacciones de los interlocutores. También hay cierto grado de irresponsabilidad en las expresiones y actitudes de algunos interlocutores, puesto que el medio parece ser más permisivo, o al menos permite esconderse con mayor facilidad a la hora de las represalias de los pares.

4. La inversa: la capacidad de manipulación se traslada de los mecanismos habituales en la sociedad (como la posición social o económica) a las habilidades de aquellos que manejan más el medio o que pueden intervenir de manera subrepticia en las comunicaciones ajenas.

5. La autonomía de la discusión: la censura previa o a posteriori de las discusiones por tratar de temas considerados inapropiados o indecentes por una comunidad ¿es válido impedir que una persona participe de una discusión sobre cuestiones que la comunidad no considera adecuadas, partiendo de que esa discusión no se realiza dentro de la comunidad?[29]

1.2. DEFINICIÓN DE COMPUTADORA.

[29]http://www.monografias.com/trabajos14/documentosinformaticos/documentosinformaticos2.shtml

Es una máquina capaz de efectuar una secuencia de operaciones mediante un programa, de tal manera, que se realice un procesamiento sobre un conjunto de datos de entrada, obteniéndose otro conjunto de datos de salida.[30]

1.2.1. EVOLUCIÓN DE LA COMPUTADORA.

a) La MARK (1937- 1944). Fue creada en la Universidad de Harvard, contando con el apoyo de la IBM, por Howard Aike, a finales de la década de los treinta y principios de la década de los cuarenta. Se trata de la primera computadora electromecánica automática. Podía llevar a cabo largas secuencias de operaciones previamente codificadas, que posteriormente eran registradas en una cinta de papel perforada y los resultados eran calculados apoyándose en las unidades de almacenamiento. Esta máquina era lenta, puesto que su funcionamiento dependía de la velocidad de sus aproximadamente 750.000 componentes.[31]

b) La ENIAC (1943- 1945). No tenía partes mecánicas y empleaba aproximadamente 18.000 bulbos. Podía efectuar hasta cinco mil operaciones por segundo y fue empleada para resolver problemas de balística y aeronáutica. Tenía la ventaja de emplear simultáneamente gran cantidad de componentes, pero era demasiado grande y se calentaba fácilmente.

---

[30] www.monografias.com/trabajos/histocomp/histocomp.shtml
[31] http://www.monografias.com/trabajos14/documentosinformaticos/documentosinformaticos2.shtml

c) La EDVAC (1945- 1952). Podía almacenar instrucciones internamente y llevar a cabo operaciones con números binarios. Fue creada por el mismo que fabricó la ENIAC.[32]

d) La UNIVAC (1951). Apareció como la primera computadora comercial. Se caracteriza por el uso de una cinta magnética para la entrada y salida de datos, además posee un programa que puede transferir programas de lenguaje particular a lenguaje de máquina.

En 1963 aparecen las computadoras de tercera generación, caracterizadas por el uso de circuitos integrados monolíticos, que produce una enorme ventaja: aumenta considerablemente la velocidad de operación, incrementa la confiabilidad y se reduce el costo y tamaño. Posteriormente, aparecen las llamadas computadoras de cuarta generación, con la integración a gran escala, la aparición de microcircuitos integrados y evidentes mejoras, entre ellas, la llamada microprogramación (firmware).[33]

1.2.2. TIPOS DE COMPUTADORAS.

Existen dos tipos de computadoras:

---

[32] PÉREZ, Luño Antonio Enrique. Manual de informática y Derecho. Editorial Ariel S.A., Barcelona, 1991. P.82-103.

[33] www.monografias.com/trabajos/histocomp/histocomp.shtml

a. Computadora Analógica.

Aprovechando el hecho de que diferentes fenómenos físicos se describen por relaciones matemáticas similares (v.g. Exponenciales, Logarítmicas, etc.) pueden entregar la solución muy rápidamente. Pero tienen el inconveniente que al cambiar el problema a resolver, hay que realambrar la circuitería (cambiar el Hardware).[34]

b. Computadora Digital

Están basadas en dispositivos biestables, i.e., que sólo pueden tomar uno de dos valores posibles: '**1**' ó '**0**'. Tienen como ventaja, el poder ejecutar diferentes programas para diferentes problemas, sin tener que la necesidad de modificar físicamente la máquina.

1.3. INFORMÁTICA.

La Informática, es el estudio del tratamiento de la información en general y, particularmente, del tratamiento automático de la información utilizando computadoras. La palabra "Informática" está compuesta por los vocablos información y automatización, y fue empleada por primera vez en el año 1962 por

[34] Tipos de computadoras: analógicas y digitales. dmoz.org/World/Espa%F1ol/Computadoras/Historia

Philipe Dreyfus.[35] Se refiere al conjunto de técnicas destinadas al tratamiento lógico y automático de la información, con el fin de obtener una mejor toma de decisiones. Surgió por el impulso del hombre del formular nuevos postulados y desarrollar técnicas que le permitieran satisfacer la creciente necesidad de información para la toma de decisiones.[36]

La palabra española "informática" deriva del vocablo francés "informatique", que a su vez es un compuesto contracto de "información" y "automatica". La informática alude directamente al tratamiento automático de la información.

En este orden de ideas, el diccionario de la Real Academia de la Lengua Española de 1984 definía la voz "informática" como el "conjunto de conocimientos científicos y técnicos que hacen posible el tratamiento automático de la información por medio de calculadoras electrónicas." Actualmente, con el avance de la técnica, ha sido preciso cambiar las palabras "calculadoras electrónicas" por "ordenadores", pero de resto la definición se ha mantenido intacta.

---

[35] PÉREZ, Luño Antonio Enrique. Manual de informática y Derecho. Editorial Ariel S.A., Barcelona, 1991..

[36] MEJAN, Luís Manuel C., El Derecho a la intimidad y la informática. 2º ed., México, Porrúa, 1996, XXII-146 p.p.

Citamos otras definiciones que nos pueden ayudar a asimilar mejor el campo propio del Derecho Informático:

Informática, es la ciencia del tratamiento sistemático y eficaz, realzado especialmente mediante máquinas automatizadas, de la información, contemplada como vehículo del saber humano y de la comunicación de los ámbitos técnico, económico y social (Documento IBI).[37]

La disciplina que estudia el fenómeno de la información, y la elaboración, transmisión y utilización de la información principalmente, aunque no necesariamente, con la ayuda de ordenadores y sistemas de telecomunicación como instrumentos (Altmark).

Informática es la aplicación racional y sistemática de la información para el desarrollo económico, social y político (Altmark). "La ciencia del tratamiento lógico y automático de la información" (Delpiazzo y Montano).

Son los aspectos de la ciencia y la tecnología específicamente aplicables al tratamiento de la información y, en particular, al tratamiento automático de datos.[38]

---

[37] MEJAN, Luís Manuel C., El Derecho a la intimidad y la informática. 2º ed., México, Porrúa, 1996, XXII-146 p.p.

[38] (Centre de Recherches Informatiques et Droit des Facultés Universitaires de Namur).

De las definiciones dadas, todas, incluso la etimológica, contienen dos elementos: "información" y "tratamiento automático". Cuando Altmark habla de "aplicación racional y sistemática" de la información, no hace sino hablar en otros términos de su "tratamiento automático". Solo varían, accidentalmente, en que unas incluyen el fin de la ciencia ("el desarrollo económico, social y político") y otras no.[39]

La informática combina los aspectos teóricos y prácticos de la ingeniería, electrónica, teoría de la información, matemáticas, lógica y comportamiento humano. Los aspectos de la informática cubren desde la programación y la arquitectura informática hasta la inteligencia artificial y la robótica. La palabra "informática" tiene un significado cada vez más tangible, más cercano para el hombre contemporáneo, lo que no significa que sea más preciso.[40] Evoca en nuestra memoria múltiples imágenes de computadoras, redes, antenas, correos electrónicos, programas de software, etc.

1.4. EL DERECHO INFORMÁTICO.

Las primeras alusiones al Derecho Informático ocurren a partir de 1949, cuando Norbert Wiener en el Capítulo IV de su obra se refiere a la influencia que ejerce la

---

[39] Jurisprudencia Argentina.-Tomo II- Año 1999- "Documento Electrónico" por Daniel Altmark, págs. 851-855.

[40] http://derecho.org/comunidad/lasalle

cibernética sobre el fenómeno jurídico. Se sugería una aparentemente imposible conjunción entre los mundos del ser y del deber ser.[41]

Ese mismo año, el Juez norteamericano Lee Loevinger publicó en la revista Minnesota Law Review un artículo titulado "The next step forward" donde señala que el próximo paso en el progreso del hombre, debe ser la transición de la Teoría General del Derecho a la Jurimetría, es decir, la investigación científica acerca de los problemas jurídicos. Cabe señalar que el estudio de las implicaciones informáticas respecto al Derecho se desarrolló en la década de los cincuenta, mientras que el estudio de las implicaciones jurídicas motivadas por la informática comienza a desarrollarse en la década de los sesenta.[42]

Por lo expresado, definimos al Derecho Informático como aquella parte del derecho que regula el tratamiento automatizado de la información. Una segunda definición la obtenemos combinando el objeto material de la ciencia, con el formal, resulta que el Derecho Informático es aquel conjunto de normas, principios e instituciones que regulan el tratamiento automatizado de la información.[43]

---

[41]http://www.monografias.com/trabajos14/documentosinformaticos/documentosinformaticos2.shtm

[42] TELLEZ Valdez, Julio. Derecho Informático, Ed. Mc. Graw - Hill México. 1997 p.56-70.

[43]http://www.monografias.com/trabajos14/documentosinformaticos/documentosinformaticos2.shtml

Concuerdan plenamente con la definición de Altmark, quien estima que "el derecho informático es el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad informática".

1.5 FUENTES DEL DERECHO INFORMÁTICO.

Tenemos a las fuentes interdisciplinarias y a las fuentes transdisciplinarias.[44]

a. Fuentes interdisciplinarias:

Son aquellas fuentes dentro de la disciplina jurídica, son fuentes propias entre las que tenemos:

1).- Legislación informática.- Son un conjunto de disposiciones, de regulaciones de normas obligatorias que regulan el mundo y las relaciones de la informática.

2).- Doctrina informática.- Es un conjunto de ideas, opiniones sobre el derecho, teorías que se elaboran sobre el tratamiento de la informática que este conjunto de opiniones puede ser teatro, libros, artículos, estudios, etc. y de estos se obtiene leyes.

3).- Jurisdicción informática.- Son los fallos, sentencias, resoluciones que tienen contenidos informáticos, en síntesis son fallos con relación a temas informáticos.

- Antes la principal fuente del Derecho fue la Costumbre.

---

[44] DAVARA Rodríguez, Miguel Ángel. Derecho Informático. España. Editorial Aranzadi, 1993.

- Hoy en día la principal fuente del Derecho es la Legislación.
- La principal fuente del Derecho Informático es la Jurisprudencia.
- **Fuentes Transdisciplinarias.**

Entre las que podemos mencionar:

1).- Sociología.- Encargada de estudiar los fenómenos que se dan en la sociedad, dando pautas de que dirección deben tomar los legisladores en las leyes referidas a la informática y su gran crecimiento.

2).- Economía.- Estudia los fenómenos económicos, y las relaciones de producción.

3).- Filosofía.- Nos indica como serán las relaciones con las normas jurídicas, nos da la señal de la ley perfecta, un prototipo de ley optimizadora para el razonamiento, la base de la informática es la lógica formal.

4).- Estadística.- Maneja datos, información, la ordena, clasifica, sistematiza, procesa, analiza, etc.

5).- Política Económica.- Si hablamos de economía política hablamos de una estrategia, de una planificación para llegar a un objetivo.

1.6. INFORMÁTICA JURÍDICA.

La Informática Jurídica es la técnica que tiene por objeto investigar los conocimientos relativos a la informática en general, y aplicarlos para recuperar información jurídica, así como para aprovechar de la mejor manera los instrumentos de análisis y tratamiento, que son necesarios para recuperar dicha información.

La Informática constituye un fenómeno-ciencia, que ha logrado penetrar en todos los ámbitos o áreas del conocimiento humano, y siendo el Derecho una ciencia, por cuanto constituye un área del humano saber, reflejándose en un conjunto de conocimientos, pues, no cae en la excepción de ser tratada por la Informática, dando lugar en términos instrumentales a la Informática jurídica, que consiste en una ciencia que forma parte de la Informática, que al ser aplicada sobre el Derecho busca el tratamiento lógico y automático de la información legal.[45]

La Informática Jurídica ha sufrido una serie de variaciones a lo largo de la evolución de la propia Informática, pero su nacimiento es demarcado en el año 1.959 en los Estados Unidos. Tuvo su comienzo cuando en los años cincuenta se desarrolla las primeras investigaciones para buscar la recuperación de documentos jurídicos en forma automatizada. De esta manera, se comienzan a utilizar las computadoras u ordenadores ya no para trabajos matemáticos, sino también para los lingüísticos. Fue en la Universidad de Pittsburg, Pennsylvania, a

---

[45] RIVERA LLANO, Abelardo, Dimensiones de la informática en el Derecho (perspectivas y problemas). Santa fe de Bogotá, Jurídica Radar, 1995, XVIII-285 p.p.

través del Health Law Center, donde el director llamado John Horty concibió la idea de crear un mecanismo a través del cual se pudiera tener acceso a la información legal de manera automatizada.[46]

Entonces, definimos a la Informática jurídica, como una ciencia que forma parte de la Informática, es la especie en el género, y se aplica sobre el Derecho; de manera que, se dé el tratamiento lógico y automático de la información legal. Es una ciencia que estudia la utilización de aparatos o elementos físicos electrónicos, como la computadora, en el Derecho. En otras palabras, es ver el aspecto instrumental dado a raíz de la Informática en el Derecho, descubriendo así las técnicas y conocimientos para la investigación y desarrollo de los conocimientos de la Informática para la expansión del Derecho, a través de la recuperación jurídica, como también la elaboración de material lingüístico legal, instrumentos de análisis, y en general el tratamiento de la información jurídica.

Es importante recordar, que la Informática jurídica como disciplina dentro de la Iuscibernética, que constituye el marco mediato entre la relación Derecho e Informática, y que la misma forma parte de la cibernética como ciencia general, han hecho posible el desarrollo de ciencias que al mezclarse posibilitan un mejor desarrollo y tratamiento de la comunicación, como se refleja en esta relación entre el Derecho e Informática de las cuales se desprenden ciertas disciplinas como

---

[46] Informática Jurídica y Derecho Informático - http://www.informatica-juridica.com/

son: la Informática Jurídica, el Derecho Informático, la Jurimetría, la Modelística Jurídica, entre otras.

CAPITULO II

EL DOCUMENTO EN GENERAL

Y SU CLASIFICACIÓN

Tradicionalmente, el medio de un documento era el papel y la información era ingresada a mano, utilizando tinta (esto es lo que se denomina hacer un documento manuscrito) o por un proceso mecánico (mediante una máquina de escribir, o utilizando una impresora láser).

En la actualidad, un documento, no solo es un escrito que contiene información. Documento es todo instrumento, escrito o no, que contiene información y que sirve para probar algo.

2.1. HISTORIA DEL DOCUMENTO.

La historia del documento constituye una hazaña tan revolucionaria como el dominio del fuego y el desarrollo de la agricultura, pues, al igual que estas otras dos, transformó profundamente la existencia humana.

Para hablar de documento, tendríamos que hablar de la escritura. La escritura es un sistema de representación gráfica de una lengua, por medio de signos grabados o dibujados sobre un soporte. Es un método de intercomunicación humana que se realiza por medio de signos visuales que constituyen un sistema. La escritura ha evolucionado a través del tiempo, primero eran grabados o dibujos

sobre piedra, arcilla, papiro, pergamino, tablas de madera cubiertas de cera y en papel.[47]

Las transacciones entre tierras alejadas y diferidas en el tiempo necesitaban plasmarse en contratos. Estos contratos consistían en unas bolas huecas de arcilla que contenían los datos, pequeñas formas de arcilla que simbolizaban los nombres de tres maneras diferentes: esferas conos y cilindro a los que se añadían unas formas convencionales que designaban aquello que se contrataba. En caso de reclamación se rompía la bola seca, sobre la cual se había firmado con su sello para su control, y en la que se comparaba la cantidad y la entrega. Estas transacciones fueron haciéndose cada vez más complejas, se podía guardar el sistema de cálculo pero tenían que acordarse de lo contratado que quedaba impreso en los sellos en los que figuraba, por medio de signos grabados en el exterior de la bola de arcilla, el contenido interior de la misma, tanto en cantidad (el número) como en calidad (las cosas contratadas). Para hacer estos signos se utilizaba una caña muy fina llamada cálamo una de sus extremidades se cortaba en forma de punta o al bies, cortando la opuesta en forma de escuadra: este era el medio para dibujar una cuña, un redondel y un cono, que representaban los datos y servía también para dibujar las formas convencionales. Finalmente se encontró la solución más simple: aplastar esta bola de arcilla y dibujar (escribir) en ambas caras el contenido del contrato: qué, cuánto, y cuando utilizando, siempre, esta

---

[47] M. ROMERO-L. RODRÍGUEZ-A. SÁNCHEZ, *Arte de leer escrituras antiguas. Paleografía de lectura*, Huelva, 1995.

pequeña caña. Es este el origen de la escritura cuneiforme (cuyo dibujo tiene forma de cuña o triangular) abandonando las formas cilíndricas y redondas.[48]

La escritura apareció hace poco más de 5.000 años. Sin embargo sus raíces, como de tantos otros inventos, se hunden en un pasado mucho más lejano. El hombre llegó a la escritura tras lentas etapas anteriores: el desarrollo del lenguaje; el descubrimiento de la representación mediante imágenes; la necesidad de reforzar la memoria almacenando información; el darse cuenta de que se podían usar tales imágenes para satisfacer esta necesidad; y por último, el difícil proceso de ensayo y error para adaptar las imágenes a la representación de los sonidos del lenguaje.[49]

El paso clave en el desarrollo de la escritura se dio cuando una imagen empezó a usarse para representar un objeto determinado, sino el sonido correspondiente a su nombre. Es la etapa de la "escritura jeroglífica", así llamada por analogía con los jeroglíficos modernos: por ejemplo, la imagen de un "sol" y la de un "dado" significan "soldado". Mediante este sistema, los signos pictográficos empezaron a ser signos fonéticos.

Este paso convirtió a la escritura en la herramienta básica de la civilización. Para las sociedades primitivas que idearon los primeros sistemas de escritura, esta

---

[48] Gelb, Ignace J. (1987) *Historia de la escritura*, Madrid ISBN 84-206-2155-2

[49] Monografias.com - Historia de la escritura

nueva herramienta significaba que las actividades humanas podían ser organizadas sistemáticamente.[50]

Además de una importante y útil herramienta práctica para el comercio y la administración, la escritura fue también una manera de reforzar un compromiso espiritual de la gente.[51] Las palabras habladas pueden tener su propio poder de sugestión, pero la escritura les añade una dimensión especial: la de la permanencia; una bendición o una maldición escritas parecían haber sido formuladas para siempre.

A partir de estos inicios iban a surgir numerosos sistemas de escritura nuevos y se iban a lograr más perfeccionamientos. El revolucionario paso hacia la escritura alfabética constituiría un salto decisivo en la expansión de la escritura y por consiguiente del documento.

Los sumerios, que se cree fueron los primeros inventores de la escritura, vivían en el sur de Mesopotamia durante el cuarto milenio antes de nuestra era.[52] Su documento escrito más antiguo se remonta al año 3.100 cuando la Revolución Urbana avanzaba ya agrandes pasos. Poco después la escritura fue reinventada por los egipcios a 1.500 kilómetros de allí. Es bastante probable que los egipcios tomaran de los sumerios la idea de la escritura, pues existen pruebas

---

[50] M. ROMERO-L. RODRÍGUEZ-A. SÁNCHEZ, *Arte de leer escrituras antiguas. Paleografía de lectura*, Huelva, 1995.

[51] Février, James G. (1995) *Histoire de l'écriture*, París ISBN 2-228-88976-8

[52] de "http://es.wikipedia.org/wiki/Escritura

arqueológicas del contacto entre ambos pueblos por esta época; pero lo único que habrían tomado sería meramente la idea, no el sistema sumerio de escritura. En primer lugar, los símbolos de la escritura egipcia son distintos de los símbolos sumerios. Las imágenes usadas en las primeras etapas de ambos sistemas difieren entre sí, incluso cuando con ellas se pretende representar un mismo objeto. Los egipcios, inventores de la escritura jeroglífica, representaban la palabra "boca" mediante un simple óvalo; en cambio los sumerios, cuya escritura dio origen a la cuneiforme, empezaron representándola dibujando una boca en un rostro barbado.[53]

Cuando el hombre primitivo comenzó a sentir la necesidad de comunicarse con los demás, lo hizo a través del lenguaje de señas, es decir, de gestos o movimientos, una comunicación inmediata. Con el tiempo aparecieron los primeros indicios de un lenguaje arcaico.

Aunque no se sabe con exactitud cuánto tiempo el hombre se limitó a estas formas de comunicación elementales, no es sino hasta quince mil años a. C. que se cree que el hombre dejó plasmadas las primeras pinturas rupestres en cavernas naturales, es decir, un dibujo esquemático de los objetos que se querían representar. Esto significó el nacimiento del dibujo y con él, el nacimiento de los signos.

---

[53] M. ROMERO-L. RODRÍGUEZ-A. SÁNCHEZ, *Arte de leer escrituras antiguas. Paleografía de lectura*, Huelva, 1995.

Estos primeros dibujos representaban ideas, mismas que a través del tiempo fueron evolucionando hasta llegar a convertirse en la representación de fonemas o fonogramas, es decir, sonidos vocales. Sin embargo, no es sino hasta el año 3100 a.C., que la historia registra los primeros trazos escritos de un hombre arcaico, en Mesopotamia. Hacia este mismo año, los sumerios dieron origen a la escritura, pues grabaron la palabra con signos; una escritura capaz de traducir, poseedora no solamente de imágenes y conceptos, sino también de sonidos, representados por signos o incisiones en forma de cuña (escritura cuneiforme).[54]

La mayoría de los textos que elaboraban los sumerios tenían que ver principalmente con el control administrativo (balances e inventarios, adquisiciones, notas de entrega, sentencias, actas, contratos, etc.). Hacia el año 2500 a. C., la escritura cuneiforme estaba lo suficientemente sofisticada como para permitir la redacción de textos literarios (mitos, epopeyas, himnos, relatos, proverbios, fábulas, etc.). Así pues, en toda la región comenzaron a surgir escuelas donde enseñaban esta escritura, que a mi modo de ver, además, era un arte.

Siglos más tarde, la escritura cuneiforme fue aprendida por diversos pueblos de Asia Menor y el pueblo semita, pueblo que permitió a los fenicios crear su alfabeto (antecedente de todos los modernos), que desarrollaron y difundieron por los países a los que llevaron su civilización (el más importante de ellos fue Grecia).

---

[54] de "http://es.wikipedia.org/wiki/Escritura

A pesar del importante aporte de los sumerios a la escritura, la escritura cuneiforme no fue el único sistema, aunque sí el más importante. Al menos siete sistemas de escritura son reconocidos por especialistas : el egipcio, el protoelemita, el protoíndico, el cretense, el hitita y el chino.

Podemos mencionar también a los códices que eran documentos antiguos.[55] Es un ejemplo de documento que recoge la tradición de la escritura indígena tradicional y la adaptación al sistema europeo. Se les clasifica dé acuerdo con sus orígenes, época, soporte, formato y contenido temático.

El soporte material para los códices prehispánicos puede ser de papel de amate, piel de venado, tela de algodón tejida en telar de cintura y posiblemente, papel de maguey; en los coloniales aparecen el papel europeo, la tela industrial y el pergamino. Más tarde surgieron reproducciones en otros materiales.[56]

En cuanto al formato existan: la tira de piel o papel de amate en composición horizontal, que recibe el nombre de banda cuando es vertical y según la manera de guardarla se llama rollo o biombo; el lienzo de tela de algodón tradicional o industrial; la hoja de papel europeo; o de amate en las dimensiones de la hoja oficial europea; el panel de piel, tela, papel indígena o europeo cuando se buscó

---

[55] ORÍGENES DEL HOMBRE. TIME LIFE. Ediciones Folio S.A. 1993

[56] http://html.rincondelvago.com/origenes-de-la-escritura.html

obtener una superficie mayor que la hoja normal uniendo varios elementos del mismo material.[57]

En cuanto el contenido temático, se ha agrupado según el tema más importante de cada manuscrito, porque casi siempre abordan varios: 1. Calendáricos - rituales (almanaques y ruedas), 2. históricos, 3. genealógicos, 4. cartográficos (lienzos, mapas y planos), 5. económicos (catastros, censos, registros financieros, planos de propiedades, tributos), 6. etnográficos, 7. misceláneos, de litigios, de historia natural, 8. catecismos indígenas y 9. Techialoyan.[58]

2.2. QUÉ ES EL DOCUMENTO.

Documento es todo instrumento, cosa o elemento material que sirve para probar algo. El documento es una cosa que hace conocer un hecho, que lo representa, por contraposición al testigo, que es una persona que narra un hecho. Siempre está presente la noción de representación que debe ser material, destinada e idónea para reproducir una cierta manifestación del pensamiento, con prescindencia de la forma en que esa representación se exteriorice.[59]

Para la Real Academia Española documentar significa "probar documentos", al mismo tiempo define como documentos "un escrito o cualquier otra cosa que pruebe o acredita algo". Este seria le Concepto general de documento.

---

[57] https://iconio.com/ABCD/F/sec_17.htm

[58] https://iconio.com/ABCD/F/sec_17.htm

[59] WIKIPEDIA, la enciclopedia libre.

La Ley de Patrimonio Histórico Español define el documento como "toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluidos los soportes informáticos.

Desde el punto de vista administrativo, documento seria toda información o hecho fijado o registrado en cualquier tipo de soporte material que sirvan para comprobar o acreditar algo.[60]

Por todo lo expuesto, documento es aquel registro incorporado en un sistema de forma escrito, video audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos.

2.3. TIPOS DE DOCUMENTOS.

Una vez consideradas las características fundamentales de los documentos podemos establecer una clasificación que parta de la consideración de dichas características. De este modo, los documentos podrían clasificarse básicamente según el tipo de soporte, la forma de su contenido y la información que ofrezcan. Además de estos puntos de vista intrínsecos, el documento también puede analizarse desde puntos de vista extrínsecos: forma de publicación, forma de utilización, grado de accesibilidad, etc. Cada una de estas categorías darán lugar a posteriores subdivisiones; especialmente el contenido puede considerarse desde

[60] www.alfa-redi.org/documento/default.asp

múltiples puntos de vista: el de la disposición, el de la materia tratada, el del grado de originalidad, etc.

Cualquier esquema de clasificación de documentos que se proponga será imperfecto y adolecerá de confusiones, no tanto por la falta de exhaustividad como por la aparente duplicidad de algunos conceptos.[61] Sin embargo, es necesario establecer una tipología determinada si se pretende llevar a cabo un análisis, por elemental que sea, de las fuentes de información.

2.3.1 SEGÚN LAS CARACTERÍSTICAS FÍSICAS:[62]

a) Tipo de material. Nos referimos al tipo de material, encontraremos:

- a los documentos de papel ya sea escrito o impreso.

- documentos de plástico los cuales se pueden moldear fácilmente.

- documentos fotográficos,

- documentos mecánicos y todos aquellos que se pueden tocar.

- documentos de vinilo y discos compactos.

b) Tamaño.

---

[61] www.surfpoint.com/Computer_Internet/Computer_Documentation/ Documentation/

[62] LAROUSSE.- Diccionario Ilustrado.- Argentina.

El formato, es decir; estilo de fuente, tamaño de fuente, el color de las letras, el subrayado, las sombras, las mayúsculas, la extensión y en cuanto al párrafo, si tendrá sangría, espacio, el nivel de esquema, viñetas, etc.

2.3.2 SEGÚN LA FORMA DE PRODUCCIÓN.-[63]

a) Manuales.

Aquellos documentos o testimonios hechos a mano.

b) Impresos.

Documentos señalados, marcados. Propiamente hablaríamos de las huellas dejadas en papel, tela, etc., las letras u otros caracteres de las formas. Como ejemplo: un periódico, un libro, folleto, revista, formulario u hojas hechos en la imprenta. Así como también, las huellas sobre una determinada cosa.

c) Mecánicos.

Su característica principal es que se utiliza las maquinas; como ser la mecanización contable, es decir, se utiliza maquinas contables para establecer documentos administrativos y comerciales.

---

[63] LAROUSSE.- Diccionario Ilustrado.- Argentina. Y WIKIPEDIA, la enciclopedia libre.

Por supuesto entran en este campo los documentos escritos a maquina.

d) Fotográficos.

Documentos fotográficos son aquellas imágenes fijadas en una placa o película, impresionables a la luz, reproducidas mediante una maquina fotográfica.

e) Magnéticos.

La que, mediante perforaciones que representan datos, puede ser leída por un ordenador o mediante una banda magnética que puede ser leída por un dispositivo electrónico, permite la realización de diferentes operaciones.

Se trata principalmente de soportes magnéticos utilizados como almacén de datos.

f) Electrónicos.

Toda representación informática, es decir; la fijación en un soporte electrónico de información, que queda registrada en la memoria auxiliar del computador. En realidad, documento electrónico en sentido restringido es el que aparece instrumentado sobre la base de impulsos electrónicos y no sobre un papel.

g) Digitales.

Aquellos documentos transformados en imágenes mediante códigos numéricos por medio de ordenadores electrónicos.

2.3.3 SEGÚN LA FORMA DEL CONTENIDO.-

a) Textuales

Aquello conforme con el texto, es decir; un escrito ya sea por un autor o en una ley.

b) Icnográficos.

Podemos hablar de estatuas, cuadros o pinturas en general. Es decir; documentos representados artísticamente donde se pueden reconocer imágenes, retratos, etc. Esto se da también en los diversos elementos: litúrgicos, dogmáticos, históricos dentro del cristianismo. Posteriormente lo mismo que con los símbolos, ocurre con las actitudes de las figuras, con la composición de las escenas u con el curso evolutivo de los temas, hasta llegar al renacimiento y a la edad contemporánea.

c) Sonoros.

Estamos hablando propiamente de los casettes, de los discos compactos. en donde se guarda cierta información publica o privada. Esta información se obtiene principalmente en las entrevistas de ciertos personajes importantes.

d) Audiovisuales.

Hablamos especialmente de documentos didácticos que se valen de grabaciones acústicas acompañadas de imágenes ópticas.

e) Plásticos.

Documentos hechos de ciertos materiales sintéticos que pueden moldearse fácilmente.

f) Informáticos

En sentido restringido documento informático, es aquella información automatizada.

g) Mixtos.

Por ejemplo: aquellos documentos que a la vez son textuales, por contener escritos; sonoros, porque producen sonidos; audiovisuales, donde guardan grabaciones acompañadas de imágenes ópticas; e informáticos guardando información automatizada…etc.

2.3.4 SEGÚN LA ESTRUCTURA DEL CONTENIDO.

a) Monografías.

La UNESCO define la Monografía como "publicación literaria no periódica de más de 48 páginas".

Martínez de Sousa admite dos acepciones: "1. Estudio especial de determinada parte de una ciencia o de cualquier otro asunto" y "2. Publicación no seriada que contiene un texto completo y homogéneo en un volumen o en un número limitado de ellos".

La norma ISO 5127-2 dice que la monografía es aquella publicación que contiene texto, ilustraciones o ambos, en forma directamente legible, que se presenta completa en un solo volumen o debe ser completada en un número finito de volúmenes y contiene un estudio detallado y completo.

Estas definiciones le suponen a la monografía al menos tres características propias: unidad de contenido, extensión finita y aparición no periódica.

Una monografía trata del estudio particular sobre un tema determinado. Entonces los documentos monográficos son aquellos que contienen un estudio profundo sobre temas determinados.

b) Publicaciones seriadas.

Martínez Sousa define la publicación seriada como "Publicación cuyos volúmenes o números se suceden regularmente en orden numérico o cronológico, con título común y con propósito de continuar indefinidamente".

Martín Vega, dice que las publicaciones seriadas son "documentos que se publican en sucesivos fascículos con una periodicidad fija o variable, no eventual como ocurre con las monografías, y desde el punto de vista del contenido, presentan una temática variopinta acerca de una o más disciplinas"

La literatura anglosajona confunde a veces el concepto de publicación seriada y publicación periódica, utilizando para ambas categorías el término periodical.

El Glosario ALA recoge la definición de las AACR2 y establece diferencias entre ambas al considerar la publicación seriada como "Publicación, realizada en cualquier soporte, que se edita en partes sucesivas, llevando el número o la fecha, o ambas cosas, y pensada para su continuación indefinida. Las publicaciones seriadas comprenden las periódicas, los diarios y revistas, anuarios e informes, memorias, actas, calendarios, etc. y las series monográficas numeradas" y la publicación periódica (*periodical*) como "Publicación en serie que aparece o se intenta que aparezca a intervalos regulares o determinados, por lo común varias veces al año, siendo cada fascículo numerado o fechado consecutivamente y suele contener artículos sueltos, narraciones y otras clases de escritos. No se incluyen en esta definición los periódicos que difunden noticias generales y las actas, documentos u otras publicaciones de entidades o corporaciones que están relacionadas con sus juntas"; El mismo sentido le concede Martínez de Sousa cuando dice que la publicación periódica es una "publicación seriada con periodicidad fija inferior a un año".

Estas definiciones acuerdan para la publicación seriada tres características básicas: aparece en fascículos ordenados, con periodicidad fija o variable, y bajo un mismo título general. Dentro de las publicaciones seriadas se diferencian las series monográficas numeradas (que pueden presentar títulos individuales diferentes bajo un título general de serie), las publicaciones periódicas y los periódicos de información general. A veces se da el caso de que las publicaciones seriadas publiquen un número monográfico que suele ser un fascículo dedicado exclusivamente a un tema determinado, pero forma parte de la colección seriada. Las publicaciones periódicas suelen ofrecer una información más actualizada que las monografías, gracias a la mayor rapidez de sus secuencias de publicación.

c) Obras de referencia.

Cuando hablamos de obras de referencia nos referimos a la colección de obras como: diccionarios, enciclopedias, manuales, anuarios, atlas geográficos, etc. Donde la persona obtiene información breve y concreta sobre cualquier concepto o tema.

2.3.5 SEGÚN EL NIVEL DE INFORMACIÓN QUE PROPORCIONAN.-

a) Primarios.

Llamamos documentos primarios o fuentes primarias a todos aquellos documentos que ofrecen información original, y reflejan los resultados directos de la investigación. El Glosario ALA los identifica como primary sources y las define

como "Documentos fundamentales, originales auténticos, que tratan una materia determinada y se utilizan en la preparación de un trabajo posterior". El sentido del término "original" se refiere a que es origen de la información y que termina en sí misma, no remite a otros documentos.

b) Secundarios.

Documentos o fuentes secundarias son todos aquellos documentos que contienen datos e información referentes a fuentes primarias. Son obras que se han elaborado a partir de otras fuentes (fuentes primarias) y no contienen información original, sino que remiten a otros documentos.

La mayoría de los documentos secundarios son fuentes de información bibliográfica propiamente dicha, ya que remiten a otros documentos originales, es decir, informan sobre documentos. Se consideran documentos secundarios las bibliografías, catálogos, índices y boletines.

c) Terciarios o documentos secundarios reelaborados.

Los documentos llamados terciarios por algunos autores y documentos secundarios reelaborados o refundidos por otros, son aquellos que remiten a documentos secundarios y son el resultado del análisis de estos. Por este motivo son el principio de cualquier búsqueda bibliográfica.

d) Complementarios.

Entre estos documentos tenemos; la cedula de identidad, el certificado de nacimiento, el certificado de matrimonio, el certificado de bautizo, la libreta militar, etc.… y todos esos documentos que forman parte de un tramite determinado.

2.3.6 SEGÚN EL GRADO DE ACCESIBILIDAD.-

a) Publicadas.

Aquellos documentos cuya característica es que son públicos, como ser: las encíclicas, constituciones, exhortaciones, cartas apostólicas, otros textos, así como también documentos oficiales del parlamento: resoluciones, decretos, leyes, reglamentos, etc.

b) Inéditas.

Los documentos inéditos, a diferencia de las fuentes publicadas, pueden llevar su contenido a científicos y especialistas más rápidamente, ya que en su preparación no media el proceso editorial. Muchas veces estos materiales llenan el vacío que dejan las publicaciones seriadas y los libros en cuanto a la satisfacción de las necesidades de información

c) Reservadas.

Los documentos reservados son los siguientes:

- Los documentos de respaldo de procesos de licitación o contratación, hasta su adjudicación o formalización del contrato.

- Los peritajes, estudios, informes técnicos e informes de derecho, respecto de materias cuyo conocimiento pueda impedir u obstaculizar gravemente el ejercicio de la acción administrativa.

- Los antecedentes o documentos o papeles de trabajo

- Los actos y documentos sobre planes de contingencia para enfrentar emergencias sanitarias relacionadas con conductas terroristas.

- Auditorias médicas de muerte o enfermedad, calificadas como reservadas por la autoridad responsable.

- Las denuncias presentadas ante los tribunales de justicia.

- Los antecedentes de los funcionarios públicos.

- Los antecedentes personales de los participantes en concursos públicos de selección de personal.

- La información relativa a las remuneraciones del personal..

- Informes evacuados por el Departamento Jurídico, Auditoria interna u otro departamento, relativos a personas determinadas o claramente identificables, requeridas en carácter de reservados por la autoridad.

- Los informes y estudios técnicos especiales, requeridos en carácter de reservados por la autoridad.

- La historia clínica de los pacientes, sin perjuicio de los derechos del paciente o su representante para cualquier información de ella, de acuerdo a la legislación vigente.

- Y todos aquellos documentos que como su nombre lo dice, son reservados.[64]

2.4. DOCUMENTOS PÚBLICOS Y PRIVADOS.

Los documentos en todas las formas se consideran frecuentemente como evidencia en procedimientos penales y civiles. Atendiendo a su origen, los documentos podemos clasificarlos en públicos y privados.

2.4.1. DOCUMENTOS PÚBLICOS.

Tomando el concepto de nuestro Código Civil[65], documento publico o autentico es el extendido con las solemnidades legales por un funcionario autorizado para darle fe pública. Cuando el documento se otorga ante un notario público y se inscribe en un protocolo, se llama escritura pública.

---

[64] Toda esta clasificación de los documentos, según a TIPOLOGIA DE LOS DOCUMENTOS de paginas Web y el Diccionario Larousse. Diccionario Ilustrado

[65] Código Civil. Libro Quinto, del ejercicio, protección y extinción de los derechos. Capitulo II, de la prueba literal y documental. Sección I, de los documentos públicos. Subseccion I.

Entonces podremos decir: documentos públicos son los autorizados por funcionarios públicos o depositarios de la fe pública, dentro de los límites de su competencia, y con las solemnidades o formalidades prescritas por la ley.

La calidad de auténticos y públicos se podrá demostrar, además, por la existencia regular en los documentos, de sello, firmas u otros signos exteriores, que en su caso prevengan las leyes.

3.4.2. DOCUMENTOS PRIVADOS.

Los documentos privados son aquellos que dejan constancia de un hecho sin solemnidad alguna, en cuyo otorgamiento no interviene un funcionario en calidad de tal, y que no llevan en si ningún sello de autenticidad.[66]

CAPITULO III

INSEGURIDAD EN LOS DOCUMENTOS

EN GENERAL

En Bolivia, la inseguridad de los documentos en general, se ha confirmado a través de los años con las falsificaciones o adulteraciones de: monedas, billetes,

---

[66] www.davara.com/documentos/relacionados.html

certificados de nacimiento, cedulas de identidad, firmas, etc. Y ahora de documentos electrónicos.

3.1. ANTECEDENTES DE INSEGURIDAD.

En la República, los hechos más trascendentales sobre falsificación, surgieron con la creación de una nueva moneda. La moneda durante la República, tenía que ser la base del crédito de la Nación y por ello se trataba de manejar este sector con cautela. Venciendo problemas, en 1829 se dispone la acuñación de moneda feble. Gobernaba el país el Mariscal Andrés de Santa Cruz, no se previeron las consecuencias que acarrearía la circulación de una moneda devaluada.

La circulación de la moneda falsa, fue tan alarmante que obligó a buscar mecanismos para disminuir los efectos. Los diferentes regímenes gubernamentales trataron de sancionar el delito de falsificación, pero no tenían éxito ni Melgarejo, Morales, Frías y Ballivián aunque estaban conscientes de que estos hechos constituían un verdadero peligro para la estabilidad del país.[67] Los casos de falsificación de moneda en la República se presentaron a veces con sutileza y habilidad, pero finalmente fueron conocidos. Entre 1843 y 1879 un periodo de 36 años se descubrieron hechos de falsificación.

---

[67] Tomas O conor D arlach/ La Republica/ editorial URQUIZO S.A./ La Paz Bolivia-1982

El interés por las monedas raras y nobles, ha despertado siempre la codicia de los especuladores dando lugar a verdaderos prodigios de falsificación y adulteración.

Conforme pasa el tiempo, hablamos ahora de Falsificaciones de tarjetas de crédito… Las primeras tarjetas de crédito aparecieron aproximadamente en la década de 1950. Con su uso surgió también la comisión de delitos en perjuicio de los propios tenedores, los comerciantes que recibían las tarjetas y las empresas emisoras.

Dinero electrónico, así se denominaban a estas piezas, del tamaño de una tarjeta de presentación, que permite comprar productos y obtener servicios cuyo pago queda diferido.[68] Las diferentes maniobras se fueron llevando a cabo y se siguen practicando aprovechando fallas en el sistema de control y seguridad (Pese a que se adoptan nuevos recaudos y se incorporan adelantos tecnológicos tendientes a detectar en tiempo oportuno el fraude) y el mismo desarrollo tecnológico que permite también anular o superar las defensas implementadas.

En consecuencia, las nuevas formas de protección, pese a ser cada vez mas sofisticadas, no han servido para impedir el fraude. Mencionaremos ahora dos delitos, afeitado y pegado; planchado y regrabado.

---

[68] Sobre el origen de los tipos de falsedad documental ver: Jakobs, loc.cit. nota 5, p.1y ss.

Afeitado y pegado**;** es la mas antigua y ya está en desuso, se realizaba a través del levantamiento mediante objetos cortantes, de los números esbozados en las tarjetas como así también el nombre del titular y su reemplazo por datos de otras tarjetas, guardando el “arte” o grafico de la tarjeta para que le confiera una apariencia de confiabilidad.

Planchado y regrabado: maniobra más evolucionada y actual que consiste en el aplastamiento de los datos embozados en los plásticos y su posterior regrabado con datos ajenos a la misma al igual que en el afeitado y pegado.

3.2. FALSEDAD DOCUMENTAL.

Es aquella información engañosa, fingida, de realidad o veracidad incierta, contrario a la verdad, es contrahacer una cosa material o inmaterial. Sin la debida seguridad y resistencia. Propiamente hablamos de un delito porque se esta cometiendo una violación a la ley.

Los delitos de falsedad presentan como denominador común que su objeto es decir, la cosa sobre la que recae la acción típica está constituido por un documento, por lo que no puede considerarse pacífico.

Tal sucede con el concepto mismo de documento en cuanto «objeto físico» y la discusión sobre su alcance (papel, cinta magnética, cinta o placa fotográfica, soporte fonográfico o visual, información recogida en ordenadores. O bien con la diferente regulación de los delitos de falsedad documental según sean creados o

cuenten con la intervención de funcionarios públicos o de particulares -aunque esa cuestión sí incide en la de la formulación de lo que ha entenderse jurídico-penalmente por documento-, ligada a la distinción entre documentos públicos y privados. También ha merecido comprensible atención doctrinal y jurisprudencial la llamada verosimilitud del documento falso o falseado, esto es, la capacidad de inducir a engaño sobre su autenticidad a un observador o lector normal.

Puesto que el concepto de documento falso debe acoger a todo soporte capaz de recoger y transportar una verdad jurídicamente relevante o probatoria, y que por supuesto es preciso que ese objeto sea capaz de engañar en cuanto a su veracidad o ausencia de manipulación.

El paso del tiempo ha reducido la casuística de las falsedades en general y de las falsedades documentales en particular solamente en una pequeña proporción, especialmente si se compara nuestro Código con los más modernos de Europa, que con unos pocos preceptos resuelven, seguramente mejor, lo que en el derecho boliviano requiere un elevado número de artículos, si se suman los específicamente dedicados a las falsedades documentales -donde ofrece hasta modalidades comitivas con aquellos relativos a falsedades específicas de documentos de crédito, papel sellado, sellos de correos, efectos timbrados y sellos y marcas, sin entrar ahora en considerar si estas «especialidades» falsarias tienen sentido «autónomo» o podrían reconducirse a una fórmula razonablemente genérica o global.

3.2.1 FALSIFICACIÓN DE MONEDA.

Como anteriormente habíamos mencionado, la inseguridad de los documentos se ha dado a través de los años, con las falsificaciones o adulteraciones de monedas, billetes, certificados de nacimiento, cedulas de identidad, firmas entre otras cosas.

En el Código Penal, en el Capitulo I, Falsificación de moneda, billetes de banco, títulos al portador y documentos de crédito, señala:

Artículo 186.- (Falsificación de moneda). El que falsificare moneda metálica o papel moneda de curso legal, nacional o extranjera, fabricándola, alterándola o cercenándola, y el que la introdujere, expendiere o pusiere en circulación, será sancionado con privación de libertad de dos a ocho años.[69]

3.2.2. DELITO DE FALSEDAD DOCUMENTAL.

En el Código Penal, en el Capitulo III, Falsificación de Documentos en General, del Titulo IV, Delitos contra la Fe Publica[70], señala:

Artículo 198.- (FALSEDAD MATERIAL). El que forjare en todo o en parte un documento público falso o alterare uno verdadero, de modo que pueda resultar perjuicio, incurrirá en privación de libertad de uno a seis años.

---

[69] Código Penal, Titulo IV, delitos contra la fe pública. Capitulo I, falsificación de moneda, billetes de banco, títulos al portador y documentos de crédito. Pág. 56.

[70] Código Penal, Titulo IV, delitos contra la fe pública. Capitulo III, falsificación de documentos en general. Pag. 59 y 60.

Artículo 199.- (FALSEDAD IDEOLÓGICA). El que insertare o hiciere insertar en un instrumento publico verdadero, declaraciones falsas concernientes a un hecho que el documento deba probar, de modo que pueda resultar perjuicio, será sancionado con privación de libertad de uno a seis años.

Artículo 200.- (FALSIFICACIÓN DE DOCUMENTO PRIVADO). El que falsificare material o ideológicamente un documento privado, incurrirá en privación de libertad de seis meses a dos años, siempre que su uso pueda ocasionar algún perjuicio.

Artículo 202.- (SUPRESIÓN O DESTRUCCIÓN DE DOCUMENTO). El que suprimiere, ocultare o destruyere, en todo o en parte, un expediente o un documento, de modo que pueda resultar perjuicio, incurrirá en la sanción del artículo 200.

Artículo 203.- (USO DE INSTRUMENTO FALSIFICADO). El que a sabiendas hiciere uso de un documento falso o adulterado, será sancionado como si fuere autor de la falsedad.

3.3. PLAGIO.

Plagio es apropiarse de la creación intelectual de otra persona, sin autorización del dueño o de quién posee los derechos sobre eso, y presentarlo como una obra propia. Hablamos de plagio, porque en Internet tenemos bastante información, así

como obras artísticas, libros, artículos, ya sean científicos, cinematográficos, películas, entonces estamos frente a muchos documentos y al ingresar a los sistemas informáticos se corre el riesgo de que alguien reproduzca, plagie, distribuya, publique.

Es decir, que cuando una persona comete plagio y que estando protegido legalmente por derechos de autor o Copyright, podría ser enjuiciado o multado. Generalmente nos referimos a plagio cuando hablamos de libros que tienen tramas o historias muy similares, a películas con semejanzas, a un invento muy similar a uno patentado, a una obra de arte similar o con alguna pieza del original o simplemente a ideas, ya que también se puede plagiar una idea.

3.3.1 DELITOS CONTRA EL DERECHO DE AUTOR.

En el Código Penal, en el Capitulo X, Delitos contra el derecho de autor, del Titulo XII, Delitos contra la propiedad[71], en el artículo 362.- (Delitos contra la propiedad intelectual), señala: quien con animo de lucro, en perjuicio ajeno, reproduzca, plagie, distribuya, publique en pantalla o en televisión, en todo o en parte, una obra literaria, artística, musical, científica, televisiva o cinematográfica, o su

[71] Código Penal, Titulo XII, Capitulo X, artículo 362, pag. 107.

transformación, interpretación, ejecución artística a través de cualquier medio, sin la autorización de los titulares de los derechos de propiedad intelectual o de sus concesionarios o importe, exporte o almacene ejemplares de dichas obras, sin la referida autorización, será sancionado con la pena de reclusión de tres meses a dos años y multa de sesenta días.

3.3.2 ARTICULO 72. MODIFICACIONES AL CÓDIGO PENAL.

En el Proyecto de Ley de documentos, firmas y comercio electrónico, en el articulo 72, modificaciones al Código Penal, en el numero 6, se añade como segundo parágrafo del articulo 362. (Delitos contra la propiedad intelectual).

“II. Incurrirá en la misma sanción quién por medios electrónicos obtenga un beneficio indebido y en perjuicio ajeno:

1) Incorpore por cualquier soporte electrónico una obra protegida por la propiedad intelectual sin la correspondiente autorización de los titulares de los Derechos de Propiedad Intelectual; o
2) Almacene definitivamente en un dispositivo interno o externo, o imprima en soporte papel una obra protegida por la propiedad intelectual sin la correspondiente autorización de los titulares de los Derechos de Propiedad Intelectual”.

3.4. MITIFICACIÓN DE INFORMACIÓN.

Empezaremos por decir que Dato, es la unidad de información y la Información es el conjunto de datos. Información es el elemento de conocimiento susceptible de ser representado con ayuda de convenciones para ser conservado, tratado o comunicado.[72] Para el Ministerio Francés de Economía y Finanzas la información es así considerada como el contenido semántico de un dato. Para la Ley Venezolana sobre Delitos Informáticos, la información es el significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

Una información, cualquiera sea su tipo o naturaleza, cuando está referida, vinculada o asociada a una persona, se transforma en un dato de carácter personal. Los medios de información proporcionan y comunican, a través de sus diversos modos de expresión, datos referidos, vinculados o asociados, a personas determinadas (o identificadas) o determinables (o identificables), y por tanto, datos de carácter personal.

Un dato personal se transforma en público, cuando el público tiene libre acceso al conocimiento del mismo. Numerosas informaciones tienen ese carácter, tales como el nombre, apellido, estado civil, etc., en tanto y en cuanto se encuentran registradas en ficheros que pueden ser accedidos por el público sin limitaciones.

---

[72] ENCARTA.- Enciclopedia electrónica. 2003

Mediante estos sistemas informáticos, la privacidad se transforma en un valor en retirada, atento a la posibilidad de conocer filiaciones políticas, pertenencia sindical, confesiones religiosas, situación patrimonial, antecedentes filia torios, amistades, preferencias de consumo, gustos y costumbres personales, etc., procesando las informaciones relacionadas con sus titulares. Cualquiera con extrema facilidad, puede llegar a conocer la historia personal de otro, y eventualmente, también sus ideas, hábitos, costumbres, amistades, etc., mediante el simple recurso de acceder al sitio en cuestión y de consignar los datos nominativos de la persona sobre la que desea indagar, y sin que esos titulares o afectados tengan la potestad de sustraer de esa forma de llegar al conocimiento de determinados hechos o circunstancias.

Con acierto se ha expresado que el avance tecnológico, especialmente en el área de la informática, abre nuevos cauces para progresos económicos, sociales y culturales, al mismo tiempo, empero, puede poner en peligro los derechos y la libertad de los individuos. Esta ambivalencia es una de las cuestiones fundamentales que debe resolver la sociedad moderna. Por un lado, el manejo y almacenamiento de grandes volúmenes de información, mediante computadoras, da lugar a una nueva fuente de poder y de desigualdad entre las personas basado en el acceso a la información. Por el otro, se acentúan las posibilidades de falsificar o mitificar aquella información contenida en los documentos.

CAPITULO IV

LOS DOCUMENTOS ELECTRÓNICOS

Y LA INSEGURIDAD JURÍDICA

En términos amplios debe entenderse por documento o instrumento a cualquier objeto que contiene una información, que narra, hace conocer o representa un

hecho, cualquiera sea su naturaleza, su soporte o continente, su proceso de elaboración o su tipo de firma. Los elementos propios de esta noción amplia, son la existencia de un soporte en que constan, un medio que se emplea para grabar los signos, un lenguaje o idioma y un mensaje o contenido.

En un sentido restringido, con la expresión documento sólo se reconocen a aquellos que están escritos en soporte papel y rubricados o firmados manualmente.

4.1. DOCUMENTO ELECTRÓNICO.

Un documento electrónico es una colección de "páginas" contenidas en un soporte electrónico que, para su visualización, requieren una pantalla gráfica o textual y unos dispositivos de emisión de sonido, según el tipo de información que contengan.[73]

Al hablarse de documentos Informáticos o electrónicos se alude a casos en que el lenguaje binario constituye la acreditación, materialización o documentación de una voluntad quizás ya expresada en las formas tradicionales, y en que la actividad de un computador o de una red sólo comprueban o consignan electrónica, digital o magnéticamente un hecho, una relación jurídica o una

[73] http://www.ucm.es/info/multidoc/prof/fvalle/tema3.htm

regulación de intereses preexistentes. Se caracterizan porque sólo pueden ser leídos o conocidos por el hombre gracias a la intervención de sistemas o dispositivos traductores que hacen comprensibles las señales digitales.[74]

Ahora bien, esbozaremos el concepto de documento electrónico, como la fijación en un soporte electrónico de información, que queda registrada en la memoria auxiliar del computador, incluyendo en este concepto los medios de recuperación de la información.[75]

En realidad, documento electrónico en sentido estricto es el que aparece instrumentado sobre la base de impulsos electrónicos y no sobre un papel. Es el conservado en forma digital en la memoria central del ordenador, o en las memorias de masa, y que no puede ser leído o conocido por el hombre sino como consecuencia de un proceso de traducción que hace perceptible y comprensible el código de señales digitales.

Sin embargo, coincidimos en que puede hablarse de documento electrónico en sentido amplio, que es el formado por el ordenador a través de sus propios órganos de salida, y es perceptible por el hombre, sin intervención de máquinas traductoras. En esta materia se ha distinguido entre los documentos introducidos

---

[74] Languages. Click for Info, Manuales y Documentos Informáticos en Castellano. Manuales y Documentos Informáticos en Castellano.
www.surfpoint.com/Computer_Internet/Computer_Documentation/ Documentation/

[75] www.acertia.com/medios/daran.html

en la memoria de base a través de la intervención humana y los introducidos por medio de una máquina (lector óptico). También se distingue en relación al documento electrónico en sentido amplio, entre la documentación (simple operación representativa) y la reproducción o repetición de la declaración del negocio. Se señala que la declaración sucesiva que naturalmente tiende a facilitar la prueba, no la produce el mismo sujeto autor de la primera, sino el ordenador, pero la misma voluntad que dio vida a la declaración precedente (que queda contenida en el ordenador) al mismo tiempo admitió que fuera plasmada en un documento elaborado por éste.[76]

Leiva, (2001)[77] define al documento electrónico como "...toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos, con eficacia probatoria o cualquier otro tipo de relevancia jurídica".

4.1.1. ELEMENTOS DEL DOCUMENTO ELECTRÓNICO.

Los documentos electrónicos poseen los mismos elementos que un documento escrito o en soporte papel:

---

[76]http://www.monografias.com/trabajos14/documentosinformaticos/documentosinformaticos2.shtml

[77] Leiva, J.(2001). El Documento Electrónico. (Documento en línea). Disponible: http//www.monografias.com/trabajos7/delec.shtml// (Consulta 2003, Abril 10).

a) constan en un soporte magnético (cintas, disquetes, circuitos, chips de memoria, redes);

b) contiene un mensaje o información, el que esta escrito usando el lenguaje convencional de los dígitos binarios o bits, entidades magnéticas que los sentidos humanos no pueden percibir directamente;

c) están escritos en un idioma o código determinado;

d) pueden ser atribuidos a una persona determinada en calidad de autor mediante una firma digital, clave o llave electrónica.

4.1.2. CARACTERÍSTICAS DEL DOCUMENTO ELECTRÓNICO.

El documento electrónico tiene las siguientes características:

a) Contiene información, porque no hay documento si no existe información.

b) Utiliza un lenguaje convencional, lenguaje que ya esta dado y es aceptado.

c) Base continente, en donde contiene la información.

d) Durable en el tiempo, es decir: que no se altere o perdure la información

e) Tiene que ser auténtico, cuando no ha sufrido alteraciones tales que varíen su contenido.

f) Identificable, el documento se debe identificar.

g) Inalterable, porque existe el temor sobre la posibilidad de reinscripción o reutilización de los soportes informáticos, puesto que disminuiría su seguridad y confiabilidad.

4.1.3. FUNCIONES DEL DOCUMENTO.

Las funciones del documento son las siguientes:

a) La de perpetuación que supone la perdurabilidad temporal;

b) la de prueba en cuanto que está destinado a acreditar la existencia de relaciones jurídicas y

c) la de garantía en cuanto que la autoría del documento se atribuye a una determinada persona, por lo que el ilícito penal habrá de atentar contra alguna de estas funciones que conformarían el bien jurídico protegido.

4.2. VALOR JURÍDICO DE LOS DOCUMENTOS ELECTRÓNICOS.

El documento electrónico, tiene un valor jurídico en cuanto a prueba se refiere. En el Código de Procedimiento Civil, en el articulo 373 (medios probatorios en general) todos los medios legales así como los moralmente legítimos aunque no especificados en este Código, serán hábiles para probar la verdad de los hechos en que se fundare la acción o la defensa. Y el artículo 374 (medios legales de prueba) son medios legales de prueba:

1) Los documentos.
2) La confesión.
3) La inspección judicial.
4) El peritaje.
5) La testificación.

6) Las presunciones.

En el Código de Procedimiento Penal, el Artículo 171 señala al respecto (libertad probatoria) el juez admitirá como medios de prueba todos los elementos lícitos de convicción que puedan conducir al conocimiento de la verdad histórica del hecho, de la responsabilidad y de la personalidad del imputado. Podrán utilizarse otros medios además de los previstos en este libro…

La prueba documental o instrumental es la que se produce por medio de documentos o instrumentos en la forma prefijada por las leyes, y es la de mayor uso en el mundo contractual y mercantil. Goza de gran confianza para el legislador en atención a la fijeza que el hecho a probar da el documento.

La prueba, es la demostración de la verdad de un hecho, y más precisamente, es la demostración, por alguno de los medios que la ley establece (Art. 1286)[78], de la verdad de un hecho del cual depende la existencia de un derecho. La prueba de los actos jurídicos es independiente de su existencia. Mientras la forma debe existir al tiempo de celebrarse el acto (por ser un elemento esencial), la prueba podrá existir desde entonces o solo posteriormente. Un acto podrá existir (y en consecuencia tendrá forma) aunque luego pueda no ser probado.

La palabra prueba tiene varias acepciones, una de las cuales se refiere a los medios de prueba, que son los elementos que la ley admite con fuerza probatoria,

[78] Código Civil, Libro Quinto. Titulo I, de las pruebas en general. Pag. 310.

es decir con aptitud para acreditar la verdad del hecho. Una especie del género medios de prueba lo constituye la llamada prueba documental, que consiste en acreditar la verdad del hecho utilizando documentos.

Podemos mencionar que la prueba es la demostración de la verdad de una afirmación, de la existencia de una cosa o de la realidad de un hecho. Cabal refutación de una falsedad. También podemos decir que es la persuasión o convencimiento que se origina en otro, y especialmente en el juez o en quien haya de resolver sobre lo dudoso o discutido.

4.3 FORMAS DE DAR VALOR PROBATORIO.

Una de las mejores formas que se esta implantando casi en todo el mundo con muy buenos resultados, e incluso talvez la única forma de dar valor probatorio a un documento electrónico es colocar una firma digital. La firma digital es condición sine qua non para la validez y eficacia del documento informático.

En la jurisprudencia se encuentra la interpretación auténtica del término y define firma digital como el resultado de un proceso informático, el cual se funda en un sistema de claves asimétricas, una pública y otra privada, cuya función principal es la evidencia o verificación del autor y la integridad del contenido del documento

mediante la autorización por el suscriptor a través del uso de su clave privada, y por el destinatario a través de su clave pública.[79]

4.4. INSEGURIDAD EN SISTEMAS INFORMÁTICOS.

Sistema informático es aquel conjunto de material y de programas comprendiendo un computador, utilizado para generar, enviar, recibir, archivar o procesar de alguna u otra forma mensajes de datos. Sistema también es cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o por interdependencia para cumplir una serie de funciones especificas, así como la combinación de dos o mas componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

Ahora bien el sistema de información es aquel utilizado para generar, procesar o archivar de cualquier forma mensajes de datos. Y el software es aquella información organizada en forma de programas de computación, procedimientos y documentación asociados, concebidos para realizar la operación de un sistema, de manera que pueda proveer de instrucciones a los computadores así como de data expresada en cualquier forma, con el objeto de que los computadores realicen funciones específicas.

---

[79] AZPILCUETA, Hermilio. Derecho Informático, Ed. Abeledo- Perrot Buenos aires Argentina, 1987. 18-30.

Es un hecho que durante la última década las intrusiones e incidentes de seguridad han crecido de manera exponencial estableciendo un escenario oscuro sobre la seguridad de las infraestructuras de computación en el mundo. En este sentido, las organizaciones han adelantado análisis de su seguridad, instalado múltiples mecanismos de protección y efectuado múltiples pruebas con el fin de mejorar las condiciones de seguridad existentes en cada uno de sus entornos de negocio. Sin embargo, dado que la seguridad completa no existe, el margen para un nuevo incidente de seguridad siempre se tiene, por tanto, cuando éste se presenta, se verifica en un alto porcentaje que las organizaciones no se encuentran preparadas para enfrentar la realidad sobre la inseguridad en sistemas informáticos.

El mundo globalizado está provocando un fenómeno de poder que desborda a los poderes políticos locales y no resulta fácil hallar paliativo a conflictos como éste en el que las acciones criminales trascienden los límites locales.

Se trata de conductas que, practicadas a través del uso personal de una computadora repercuten en el ámbito socio jurídico, algunas no sólo afectan al patrimonio privado (compras electrónicas utilizando datos de una tarjeta ajena por ejemplo) .y en otros casos hasta afecta patrimonios nacionales y/o bien causan daños de otra especie no susceptibles de valoración económica.

Entre los problemas de seguridad más frecuentes, están, el fraude informático, robo de software, sabotaje y vandalismo de datos, alteración, acceso y uso

indebido de datos informáticos, apropiación indebida de información confidencial propiedad intelectual, datos financieros o registros médicos, abuso de privilegios de Internet, virus informáticos, manipulación informática, parasitismo informático etc.

4.5. CRIMINALIDAD INFORMÁTICA.

Para hablar de criminalidad, no debe olvidarse que la única que contiene la definición de delito es la ley penal y si no se observa esta premisa se caerá en imaginar que cualquier conducta cometida a través de una computadora sea como picardía o como demostración de habilidad, o la calidad de ser simplemente un experto en informática podrían llegar a constituir factores que los encuadre en una "clase criminal" debido a que no se parte en el análisis de un adecuado concepto de delito.

Dado que es profusa la literatura sobre los denominados delitos informáticos, ha menester encarar desde el punto de vista criminológico, el estudio sobre la perpetración de conductas que, sucedidas o no a través de la red, pueden llegar a constituir ilícitos penales, de existir una legislación que así los contemple. Ahora bien, nace una nueva forma de criminalidad, con características propias de la nueva era, como ser falsificación de documentos o alteración, destrucción, etc.

Toda conducta típica, antijurídica y culpable que sea vea facilitada o convertida en más dañosa o más lucrativa a causa de la vulnerabilidad creada por el uso

creciente de los sistemas informáticos.[80] En la delincuencia informática, el computador puede fungir como objetivo de la acción dañosa (como, por ejemplo, en el sabotaje informático) o bien como mero instrumento para su comisión (como, por ejemplo, en el fraude informático).

4.6. DELITOS INFORMÁTICOS.

Toda acción antijurídica culpable realizada por un ser humano mediante medios electrónicos, magnéticos o telemáticos.

Por supuesto son aquellas actitudes ilícitas o comportamiento criminal en que la computadora esta involucrada como instrumento o fin.[81]

Una noción genérica del delito informático es la que da Antonio Enrique Pérez Luño, en Ensayos de Informática Jurídica, al afirmar que son el "conjunto de conductas criminales que se realizan a través del ordenador electrónico, o que afectan al funcionamiento de los sistemas informáticos".[82]

4.6.1. SABOTAJE INFORMÁTICO.

En lo referente a Sabotaje Informático podemos encontrar dos clasificaciones las cuales son las siguientes:

a. Conductas dirigidas a causar daños físicos

---

[80] Delitos Informáticos - http://delitosinformaticos.com

[81] Ciberderecho - http://www.geocities.com/SiliconValley/Circuit/4888/index.htm

[82] Antonio Enrique Pérez Luño. Ensayos de Informática Jurídica

Esto es cuando la persona que comete el delito causa daños físicos al hardware del equipo objeto del delito[83].

Esto puede ocurrir de varias formas, por ejemplo:

- Uso de instrumentos para golpear, romper o quebrar un equipo de cómputo, ya sea el daño completo o parcial.
- Uso de líquidos como café, agua o cualquier líquido que se vierta sobre el equipo y dañe las piezas y componentes electrónicos.
- Provocar apagones o cortos en la energía eléctrica con intención de causar daños en el equipo.
- Utilizar bombas explosivas o agentes químicos que dañen el equipo de cómputo.
- Arrancar, o quitar componentes importantes de algún dispositivo del equipo, como CD-ROM, CD-RW, Disco de 3 ½, Discos Duros, Impresoras, Bocinas, Monitores, MODEM, Tarjetas de audio y video, etc.

Y cualquier otra forma que dañe la integridad del equipo de cómputo.

---

[83] Delitos Informáticos - http://delitosinformaticos.com

b. Conductas dirigidas a causar daños lógicos.[84]

Esto comprende los daños causados a la información y todos los medios lógicos de los cuales se vale un Sistema de Cómputo para funcionar adecuadamente.

Por ejemplo, dañar la información contenida en unidades de almacenamiento permanente, ya sea alterando, cambiando o eliminando archivos; mover configuraciones del equipo de manera que dañe la integridad del mismo; atentar contra la integridad de los datos pertenecientes al dueño del equipo de cómputo y todas aquellas formas de ocasionar daños en la parte lógica de un sistema de cómputo.

-Medios Utilizados para Realizar Daños Lógicos:

Virus. Es una serie de claves programáticas que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

Gusanos. Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan

[84] http://www.delitosinformaticos.com/

graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.

Bomba Lógica o cronológica. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

4.6.2. FRAUDE A TRAVÉS DE COMPUTADORAS. [85]

Cuando la computadora es el medio para realizar y maquinar fraudes por una persona, se considera un delito.

a. Manipulación de los datos de entrada

[85] http://www.delitosinformaticos.com/

Este tipo de fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

b. Manipulación de Programas[86]

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

c. Manipulación de los datos de salida

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de

---

[86] http://www.monografias.com/trabajos6/delin/delin2.shtml

adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas, sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

d. Otro ejemplo común.

Por ejemplo, cuando una persona tiene acceso a una base de datos de nóminas de una empresa, y tiene la capacidad y autorización para manipular los sueldos de los empleados, esta persona tiene la oportunidad de cometer un delito al tomar la fracciones pequeñas de los centavos y manipularlas de tal manera que las manda a su cuenta y así obtener ganancias deshonestas lo que sería un fraude.

Una posible manera de tener mas control sobre este tipo de actos, sería designar a un grupo encargado de la administración de las nóminas de los empleados de la empresa y que ese grupo se encargue de mantener todo bajo control, revisando muy bien cada movimiento que se realice y a donde se esta enviando el dinero, porque de esta manera ya son mas personas y no es una sola que podría hacerlo sin que nadie se de cuenta, así habría menos probabilidades de que se cometa el incidente.

4.6.3. ESTAFAS ELECTRÓNICAS.[87]

El hacer compras en línea mediante el uso de Internet o alguna red de servicio, y no cumplir con lo establecido en el acuerdo de compra, en entregar el producto de forma completa o parcial, se considera fraude, lo que es muy común al hacer compras por Internet donde se requiere pagar a la cuenta de alguna persona antes de recibir el pedido.

Las personas que se dedican a este tipo de estafas, consiguen clientes, gente que se interese en comprarles el producto que venden y cuando esas personas se deciden por hacer la compra y pagan a la cuenta que se les dio, ya no se entrega nada pues lograron engañar a todas esas personas.

También aquellos lugares o sitios donde se hacen citas, ofrecen cosas que luego no son verdad, son estafas electrónicas. Lo que hace que no se pueda tener la suficiente confianza para hacer las compras en línea.

Por lo que lo mejor sería limitarse a hacer las compras solo en aquellos lugares que están garantizados y son conocidos. Hay que evitar aquellos que son sospechosos o que no son conocidos y no dan confianza, porque ahí se podría generar una estafa.

---

[87] http://www.delitosinformaticos.com/

4.6.4. PESCA U OLFATEO DE CONTRASEÑAS.[88]

Hacer uso de programas o métodos que puedan descifrar claves o que puedan averiguar o buscarlas. Ya sean claves personales de una cuenta de correo electrónico, contraseña para entrar al sistema, claves de acceso a algún sitio, claves de productos, etc.

Para poder evitar un poco esto, se recomienda que las claves no sean muy obvias, teniendo como respuesta el nombre de una persona familiar, o el de la mascota de esa persona, fecha de nacimiento, o frases que use comúnmente. También es importante cambiar periódicamente las contraseñas para que así no sea siempre una posibilidad de descifrar la contraseña.

4.6.5. COPIA ILEGAL DE SOFTWARE.

Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un *delito informático* debido a que el bien jurídico a tutelar es la propiedad intelectual.

---

[88] http://www.delitosinformaticos.com/

4.6.6. ESPIONAJE INFORMÁTICO.

El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

4.6.7. INFRACCIÓN DEL COPYRIGHT EN BASES DE DATOS.

Es la infracción de los derechos reservados del autor, ya que todo producto de marca tiene sus derechos y el infringir y violar la información de las bases de datos, ya sea ver, copiar, borrar, alterar es también un delito.

4.6.8. USO ILEGITIMO DE SISTEMAS INFORMÁTICOS AJENOS.

El usar un Sistema Informático de manera prohibida o incorrecta fuera del propósito para el que fueron creados, o para obtener ganancias a su autor o solo por cometer actos ilegítimos en contra de alguien o algún Sistema.

4.6.9. ACCESOS NO AUTORIZADOS.

El acceder a información, sitios o secciones que no están autorizadas a usuarios comunes sino solo a aquellos que tienen autorización. Acceso indebido. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años de cárcel.[89]

4.7. INSEGURIDAD EN INTERNET.

Internet es un 'sistema global de información que:

a) se encuentra lógicamente interconectado por direcciones únicas globales basadas en el Protocolo Internet (IP) o sus consecuentes extensiones;

b) es posible soportar comunicaciones haciendo uso del Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP) o sus consecuentes extensiones, y/u otro IP -compatibles protocolos y

c) provee o hace accesible, privadamente, un alto nivel de servicio basado en las comunicaciones o infraestructuras descriptivas. Se trata de 'una red internacional de computadoras interconectadas"La 'International Network of Comuters'

---

[89] http://www.monografias.com/trabajos6/delin/delin2.shtml

(Internet), se encuentra constituida 'por una red de redes de computadores unidos por líneas telefónicas, fibras ópticas, cables submarinos y enlaces por satélite que vinculan Universidades, Gobiernos, empresas y millones de individuos en casi todo el mundo'. Una página Web puesta en la red, a través de ese sistema de computadoras interconectadas, puede ser accedida y conocida por cualquier persona que se conecte conociendo la dirección de Internet de la misma. Si el acceso no se encuentra restringido, cualquier usuario del mundo puede acceder a dicha página y a su contenido.

El ciberespacio es un mundo virtual en el que los defectos, miserias y malos hábitos del ser humano se reproducen con la mayor fidelidad que las virtudes. El efecto de aldea global generado por el entramado de redes y la proliferación de nodos en todo el planeta ayudan a la difusión inmediata de los mensajes y permite el acceso a cualquier información introducida en la red.

El delito por Internet es fácil de realizar por el anonimato; por ejemplo, cuando realizamos un contrato electrónico, como en el caso de las compras telemáticas se corre el riesgo de engañar, de estafar. Actualmente se está produciendo un intenso debate respecto a la necesidad de prevenir y sancionar estos malos usos en la red de redes, Internet.

A pesar de que el concepto de delito informático engloba tanto los delitos cometidos contra el sistema como los delitos cometidos mediante el uso de sistemas informáticos, cuando hablamos del ciberespacio como un mundo virtual

distinto a la vida real, nos referimos al delito informático como aquél que está íntimamente ligado a la informática o a los bienes jurídicos que históricamente se han relacionado con las tecnologías de la información: datos, programas, documentos electrónicos, dinero electrónico, información, etc.

4.8. INSEGURIDAD DEL DOCUMENTO ELECTRÓNICO.

Es un hecho ya, que el intercambio de información de forma electrónica está inserto en la sociedad, porque el mundo avanza de forma acelerada en todo cuanto tiene que ver con el desarrollo de tecnologías de información y comunicaciones, surgiendo nuevas formas de trabajar, aprender, comunicarse y celebrar negocios; borrando fronteras y acortando distancias.

Y estas nuevas formas de interacción cuentan con millones de usuarios en el mundo entero, lo que necesariamente trae incidencias en todos los aspectos del quehacer humano, ocasionando que personas y empresas se sientan inseguras de efectuar transacciones de esta manera, por la incertidumbre que esto genera; inclusive, en algunos casos, son los mismos Jueces quienes cuestionan la eficacia probatoria de los documentos y acuerdos que no constan en papel, precisamente porque se corre el riesgo de que los documentos electrónicos sean manipulados, alterados, modificados, destruidos, por el libre acceso a los sistemas informáticos o simplemente por conectarnos a Internet.

Cuando nos conectamos a Internet, tenemos acceso a todo tipo de información, se puede enviar mensajes o documentos importantes mediante el correo electrónico, pero muchos ordenadores pueden ver dicha información. Aunque existen programas que proporcionan un alto grado de confidencialidad en el correo por ejemplo, no se puede garantizar una completa seguridad.

Ahora bien, el documento electrónico, puede ser definido como un medio de expresión de la voluntad, mediante el cual se crean, modifican o extinguen derechos y obligaciones por medio del uso de la Electrónica, Informática o de la Telemática, pero precisamente porque se trata de un documento que crea, modifica y extingue derechos y obligaciones, es que existe inseguridad jurídica. Inseguridad en cuanto a la veracidad y autenticidad del contenido del documento, inseguridad en cuanto a su validez como documento probatorio.

Lamentablemente nuestro derecho positivo no contempla expresamente su regulación. Pero, además de ello, problemas tales como la actuación por intermediarios, la constancia fidedigna de la representación que ostentan y la desconfianza que genera la autenticidad de los documentos, debido a la posibilidad de ser manipulados, no necesariamente intencionadas de los mismos, son temas aún no resueltos satisfactoriamente. Por lo que se hace necesario proteger a los documentos electrónicos, mediante una normativa integral, otorgando seguridad, de manera que sea posible emplear éstos como medio probatorio en cualquier procedimiento, bien sea administrativo o judicial.

Tal y como ya se señaló, es innegable que el intercambio de información de forma electrónica está inserto en la Sociedad, lo que hace necesario que se realicen modificaciones en las normas jurídicas y se cuente con la tecnología idónea para reconocer los acuerdos celebrados de forma electrónica y poder emplear éstos como medio probatorio en cualquier procedimiento.

En los países donde se acepta el sistema de libre apreciación de la prueba, los Jueces para la valoración de las mismas recurren al análisis de elementos presentes en estas tales como integridad, inalterabilidad, veracidad y exactitud. Es innegable que los documentos electrónicos pueden llegar a cumplir e incluso a superar estos requisitos, sobretodo en cuanto a integridad e inalterabilidad, sin embargo los sistemas informáticos son tan inseguros, por que existen programas o métodos que pueden descifrar claves.

Por eso, que se hace imprescindible que tanto los estudiantes como los profesionales del Derecho y aún más, los Jueces y Funcionarios del Sistema Judicial cuenten con una preparación técnica que les permita comprender los límites y capacidades de toda esta tecnología, que empleen con facilidad y sin complicaciones aquellos instrumentos con los cuales ocurre todo este flujo de información, tales como procesadores, y que conozcan y entiendan términos como mensajes de datos, firmas electrónicas, documentos y certificados electrónicos y otros; de manera que puedan establecer una adecuada valoración de estos

medios para luego crear una legislación que nos otorgue seguridad para realizar ciertos actos jurídicos, así como la contratación y el comercio electrónico, que representan una nueva forma de expresar la voluntad de las partes, producto del desarrollo de la tecnología, en búsqueda de facilitar la transmisión de mensajes y agilizar las transacciones jurídicas comerciales.

Es necesario decidir pronta y prudentemente para que cuando estos medios sean presentados en juicio, sean respaldados y admitidos teniendo la certeza de que no han sido modificados, alterados, falsificados, o destruidos También se hace imprescindible la capacitación técnica a todas aquellas personas vinculadas al Derecho, como ya se señaló, de manera que puedan sentirse seguras al emplear estos medios.

Lo que la inseguridad jurídica de los documentos electrónicos anticipa una serie de problemas por que se trata de casos en los que se debe proteger e inducir a la confianza de las personas, se debe otorgar la certeza de que sus actos por siempre serán validos.

4.9. INSEGURIDAD EN LOS CONTRATOS ELECTRÓNICOS.

El contrato electrónico, es aquél acuerdo de dos o mas voluntades para crear o transmitir, modificar o extinguir derechos y obligaciones, que se realiza mediante la utilización de algún elemento electrónico cuando éste tiene o puede tener una

incidencia real y directa sobre la formación de la voluntad o el desarrollo de la interpretación futura del acuerdo.[90]

Como ya mencionamos anteriormente existe mucha inseguridad en los sistemas informáticos en general y por lo tanto cuando realizamos contratos mediante medios electrónicos, estaríamos hablando de inseguridad.

Lo que distingue un contrato tradicional respecto de un contrato electrónico es, tan sólo, la formación del mismo, la forma de prestación del consentimiento, de perfección del negocio y, en consecuencia, su prueba, tanto judicial como extrajudicial.

Un marco jurídico propio debe de reconocer su propio ámbito de aplicación y protección. Un marco jurídico propio debe de regular de forma prioritaria y principal el documento electrónico como forma esencial y soporte probatorio de los negocios jurídicos concluidos electrónicamente, en definitiva, como una cautio o seguridad de la sociedad.

Si históricamente el documento ha sido identificado como escrito (prueba literal), sobre todo por la doctrina notarial, en la actualidad, "el concepto de documento

---

[90] PACHECO ESCOBEDO, Alberto, “La contratación por medios electrónicos”, en Homenaje a Manuel Borja Martínez. México, Porrúa, Colegio de Notarios del Distrito Federal, 1992, pag. 207 a 231.

trasciende al de simple escrito". Si lo normal es la presentación de escritos como prueba en un proceso, el avance tecnológico, que ha conducido a la tecnificación de las relaciones humanas, ha hecho posible otras formas documentales distintas de los simples escritos.

Por este motivo, debe existir un marco jurídico de protección. Se debería tener en cuenta algunos pasos técnicos que deben darse para celebrar un contrato, tomando en cuenta los medios técnicos para identificar y corregir los errores de introducción de datos antes de ejecutar el pedido. Por ejemplo como ocurre con las tarjetas de crédito, tarjetas de debito, cheque electrónico, pago por e-mail.

Julio Téllez Valdez habla de los siguientes acuerdos contractuales: contratos de material o de sistema; compatibilización de equipos y programas; servicios y aprovisionamiento de refacciones; contratos de programa-producto; adquisición de programas; licencia de uso de programas; desarrollo de programas; análisis y tratamiento de datos; contrato de mantenimiento; contrato de asesoría; y contrato de formación y capacitación. A su vez Olivier Hance, en Leyes y negocios en Internet, enumera los siguientes contratos: de proveedor de acceso a Internet; de operador de sistema en Internet; de suministro de información; de publicación en Internet; de renta de espacios en línea y servicios relacionados; de publicidad en línea; de correduría en línea; para la renta de espacio publicitario en línea; de desarrollo de productos multimedia en línea; de encuestas de mercado en línea; de distribución en línea; de desarrollo y mantenimiento de una página Web; de

investigación en línea; de cabildeo y mercadotecnia en línea; de participantes en un foro en línea; para acceso a bases de datos en línea; contrato maestro de ventas al menudeo; contrato de comercio electrónico entre profesionales; contrato de certificación de autoridad; y política de uso aceptable, etc.

En la Ley Modelo de Comercio Electrónico, en el Capitulo IV, Contratación Electrónica, señala:

Artículo 26 (Validez de los contratos electrónicos)

I. Los contratos civiles, comerciales y de otra naturaleza previstos en normas generales y especiales nominados o innominados, podrán ser instrumentados mediante documentos electrónicos. A ese fin, podrá tenerse en cuenta las regulaciones contenidas en los artículos 491, 492 y 493 del Código Civil vigente. No se negará efectos jurídicos, validez o fuerza obligatoria a un contrato, a las manifestaciones de voluntad u otras declaraciones por la sola razón de estar en forma de uno o más mensajes de datos.

II. Lo dispuesto en el presente Capítulo no será aplicable a aquellos contratos en los cuales la Ley excluya expresamente la validez de los mensajes de datos.

Artículo 27 (Formación del contrato)

En el marco de lo determinado por los artículos 455 y 462 del Código Civil y artículo 816 del Código de Comercio, si las partes no convinieran otra cosa, la

oferta, contraoferta y su aceptación podrán ser expresadas por medio de mensajes de datos.

Artículo 28 (Perfeccionamiento)

I. La formación del consentimiento en los actos jurídicos se producirá cuando el iniciador reciba la aceptación del destinatario, mediante el envío del correspondiente mensaje de datos y se entenderá que el acto se ha perfeccionado en el lugar de la oferta o de la oferta modificada; si hubiera acuerdo especial, se tendrá como lugar de perfeccionamiento el que acordaren las partes.

II. El perfeccionamiento de los contratos electrónicos se someterá en todo lo que fuere aplicable a los requisitos y solemnidades previstos en las normas aplicables.

III. La recepción, confirmación de recepción, o apertura del mensaje de datos, no implica aceptación del contrato electrónico, salvo acuerdo de las partes.

CAPITULO V

MECANISMOS DE SEGURIDAD

PARA LOS DOCUMENTOS ELECTRÓNICOS

Seguridad, es la certeza que se tiene sobre algo. Seguridad, es la condición que resulta del establecimiento y mantenimiento de medidas de protección, que garanticen un estado de inviolabilidad de las influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas, o que afecten la operatividad de las funciones de un sistema de computación.[91]

Sin embargo, en los últimos decenios va creciendo la impresión de que la tecnología es un factor importante de inseguridad. Para esto tendríamos que aplicar técnicas de seguridad informática para reducir los riesgos e implementar controles, ó tomar medidas correctivas.

---

[91] CANO, J. (2004) Hacia un concepto extendido de la mente segura. Pensamiento sistémico en seguridad informática. Artículo de investigación (En revisión). Universidad de los Andes

Aquí algunos mecanismos de seguridad para los documentos electrónicos, pensaremos en las medidas criptográficas, claves de cifrado, control de accesos, políticas y estándares de seguridad, mecanismos de autenticación y control, seguridad en bases de datos, y notarios electrónicos.

5.1. LA CRIPTOGRAFÍA.

La criptografía es un método o instrumento para ocultar información y da protección y seguridad a los documentos electrónicos.

La criptografía (del griego kriptos, "ocultar", y grafos, "escribir", literalmente "escritura oculta") es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos. Es decir, se la define como el "Arte de escribir con clave secreta o de un modo enigmático",... de modo que sea imprescindible aquélla para descifrar lo escrito.[92]

Con más precisión, cuando se habla de esta área de conocimiento como ciencia se debería hablar de criptología, que engloba tanto las técnicas de cifrado, la criptografía propiamente dicha, como sus técnicas complementarias: el criptoanálisis, que estudia los métodos que se utilizan para romper textos cifrados con objeto de recuperar la información original en ausencia de la clave.[93]

---

[92] Miguel Ángel Gallardo Ortiz

[93] -Estrategias de Seguridad. Benson Christopher (Inobis Consulting Pty Ltd). Microsoft© Solutions. Noviembre 2000. http://www.microsoft.com/latam/technet/articulos/200011

Otro método utilizado para ocultar el contenido de un mensaje es ocultar el propio mensaje en un canal de información, pero en puridad, esta técnica no se considera criptografía, sino esteganografía. Por ejemplo, mediante la esteganografía se puede ocultar un mensaje en un canal de sonido, una imagen o incluso en reparto de los espacios en blanco usados para justificar un texto. La esteganografía no tiene porqué ser un método alternativo a la criptografía, siendo común que ambos métodos se utilicen de forma simultánea para dificultar aún más la labor del criptoanalista.[94]

En la actualidad, la criptografía no sólo se utiliza para comunicar información de forma segura ocultando su contenido a posibles fisgones. Una de las ramas de la criptografía que más ha revolucionado el panorama actual de las tecnologías informáticas es el de la firma digital: tecnología que busca asociar al emisor de un mensaje con su contenido de forma que aquel no pueda posteriormente repudiarlo.

En la jerga de la criptografía, la información original que debe protegerse se denomina texto en claro. El cifrado es el proceso de convertir el *texto plano* en un galimatías ilegible, denominado texto cifrado o criptograma. Por lo general, la aplicación concreta del algoritmo de cifrado (también llamado cifra) se basa en la existencia de una clave: información secreta que adapta el *algoritmo de cifrado*

---

[94] -Really. http://www.securecoding.org/

para cada uso distinto.[95] Las dos técnicas más básicas de *cifrado* en la criptografía clásica son la sustitución (que supone el cambio de significado de los elementos básicos del mensaje -las letras, los dígitos o los símbolos-) y la transposición (que supone una reordenación de las mismas); la gran mayoría de las *cifras* clásicas son combinaciones de estas dos operaciones básicas. El descifrado es el proceso inverso que recupera el *texto plano* a partir del *criptograma* y la *clave*. El protocolo criptográfico especifica los detalles de cómo se utilizan los *algoritmos* y las *claves* (y otras operaciones primitivas) para conseguir el efecto deseado. El conjunto de *protocolos*, *algoritmos de cifrado*, procesos de gestión de claves y actuaciones de los usuarios, en su globalidad es lo que constituyen un criptosistema, que es con lo que el usuario final trabaja e interactúa.

Existen dos grandes grupos de *cifras*: los algoritmos que utilizan una única *clave* tanto en el proceso de *cifrado* como en el de *descifrado* y los que utilizan una *clave* para *cifrar* mensajes y una *clave* distinta para *descifrarlos*. Los primeros se denominan cifras simétricas o de clave simétrica y son la base de los algoritmos de cifrado clásico. Los segundos se denominan cifras asimétricas, de clave asimétrica o de clave pública y clave privada y forman el núcleo de las técnicas de cifrado modernas.[96]

---

[95] CANO, J. (2000) *Programación Segura? Conceptos y Aspectos Técnicos*. Conferencia Magistral. Congreso Nacional de Estudiantes de Ingeniería de Sistemas. Santafe de Bogotá. Colombia. Universidad Distrital.

[96] -Schneier, Bruce. Criptograma. Edición mensual kriptopolis.org. Marzo 1999-Julio 2001. http://www.kriptopolis.org/criptogram

Con frecuencia los procesos de cifrado y descifrado se encuentran en la literatura como encriptado y desencriptado, aunque ambos son neologismos todavía sin reconocimiento académico. Hay quien hace distinción entre "cifrado/descifrado" y "encriptado/desencriptado" según esté hablando de criptografía simétrica o asimétrica, pero la mayoría de los expertos en el mundo académico prefiere evitar ambos neologismos.

Como ya mencionamos la palabra Criptografía proviene etimológicamente del griego Kruiptoz (Kriptos-Oculto) y Grajein (Grafo-Escritura) y significa "arte de escribir con clave secreta o de un modo enigmático"[97].Aportando luz a la definición cabe aclarar que la Criptografía hace años que dejó de ser un arte para convertirse en una técnica (o conjunto de ellas) que tratan sobre la protección (ocultamiento ante personas no autorizadas) de la información. Entre las disciplinas que engloba cabe destacar la Teoría de la Información, la Matemática Discreta, la Teoría de los Grandes Números y la Complejidad Algorítmica.[98]

5.1.1. FUNCIONES DE LA CRIPTOGRAFÍA.

La finalidad de la criptografía es, en primer lugar, garantizar el secreto en la comunicación entre dos entidades (personas, organizaciones, etc.) y, en segundo lugar, asegurar que la información que se envía sea auténtica en un doble sentido:

---

[97] GONZÁLEZ, Miguel F. DANTOWITZ, Roberto. RUGNA, Daniel. Monografía "Seguridad en Internet". Facultad de Ingeniería. UBA. Primer cuatrimestre 1998. Buenos Aires. Argentina. http://cactus.fi.uba.ar/crypto/tp_ant.html

[98] MARTINO, Sergio Gustavo. Seguridad Informática By KEKO®.

que el remitente sea realmente quien dice ser y que el contenido del mensaje enviado, habitualmente denominado criptograma, no haya sido modificado en su tránsito.

Entonces la criptografía, cumple las siguientes funciones:

a) Confidencialidad,

b) Integridad del documento.

c) Autenticidad del documento

Así, la Criptografía es la ciencia que consiste en transformar un mensaje inteligible en otro que no lo es (mediante claves que sólo el emisor y el destinatario conocen), para después devolverlo a su forma original, sin que nadie, que vea el mensaje cifrado, sea capaz de entenderlo. El sistema criptográfico utiliza dos claves diferentes: Una clave pública y una clave privada.[99]

De esta manera, si utilizamos la CRIPTOGRAFÍA, tendremos la certeza de que nuestros documentos no estarán expuestos a ser modificados, alterados, falsificados, etc.…

5.1.2. CLAVE PÚBLICA.

[99] SCHNEIER, Bruce. Criptograma. Edición mensual kriptopolis.org. Marzo 1999-Julio 2001. http://www.kriptopolis.org/criptogram

En la elaboración de una firma digital y en su correspondiente verificación se utilizan complejos procedimientos matemáticos basados en criptografía asimétrica (también llamada criptografía de clave pública).

La clave pública es conocida por todos o susceptible de ser conocida, esta destinada a hacerse pública, además cumple una función técnica, cual es el cifrado del mensaje mediante el uso de la clave pública del destinatario.

La importancia de la clave pública radica en que por la misma se verifica la firma digital y, como ha sido expuesto, es prueba de la autoría e integridad del documento electrónico .Una clave es pública, que efectivamente se publica y puede ser conocida por cualquier persona.

5.1.3. CLAVE PRIVADA.

Denominada clave privada, se mantiene en absoluto secreto, ya que no existe motivo para que nadie más que el autor necesite conocerla, y aquí es donde reside la seguridad del sistema.

La clave privada, es conocida solo por el titular, cumple la función de desciframiento del mensaje por parte del destinatario. La importancia de la clave privada, viene avalada por que es generadora de la firma digital, es decir, el autor ha de firmar digitalmente el documento mediante su clave privada , la cual lleva

asociada una clave pública, si bien, ésta ha de estar vigente, es decir, no vencida, revocada o, en caso de duda, pendiente por certificar digitalmente .[100]

Como es obvio, dada su naturaleza, la clave privada solamente es conocida por el titular de la misma. Dado que la firma digital se genera a partir de la clave privada del autor, se produce una asociación entre la clave privada y firma digital que trae como consecuencia que el autor no pueda negar su firma, pues sólo él conoce la clave privada. Pero, además de esta evidencia o presunción, prevé la posibilidad, como cautela en caso de conflicto, de que la clave privada esté depositada en forma secreta ante un notario o funcionario público autorizado de tal forma que en cualquier momento puedan compararse la firma digital de un documento y la clave privada la cual lleva asociada una clave pública.[101]

Como ya dijimos la clave privada es aquella que sólo es conocida por el titular del par de claves, y que es usada para añadir una firma digital a un documento electrónico, o para desencriptar un documento electrónico previamente encriptado por medio de la correspondiente clave pública. Ambas claves son generadas al mismo tiempo con un algoritmo matemático y guardan una relación tal entre ellas

---

[100] -Anonimo. Maximum Security. A Hacker's guide to protecting your Internet Site and Network. Macmillan Computer Publishing©. 1999. EE.UU. http://sams.net –

[101] -ArCERT. Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública. Manual de seguridad en redes. Argentina. 2000. http://www.arcert.gov.ar

que algo que es encriptado con la pública, el único camino conocido para desencriptarlo es poseer la privada.

En un sistema criptográfico asimétrico, cada usuario posee un par de claves propio. Estas dos claves, llamadas clave privada y clave pública, poseen la característica de que si bien están fuertemente relacionadas entre sí, no es posible calcular la primera a partir de los datos de la segunda, ni tampoco a partir de los documentos cifrados con la clave privada. El sistema opera de tal modo que la información cifrada con una de las claves sólo puede ser descifrada con la otra. De este modo si un usuario, cifra determinada información con su clave privada, cualquier persona que conozca su clave pública podrá descifrar la misma. En consecuencia, si es posible descifrar un mensaje utilizando la clave pública de una persona, entonces puede afirmarse que el mensaje lo generó esa persona utilizando su clave privada (probando su autoría).

La clave privada es imprescindible para descifrar criptogramas y para firmar digitalmente, mientras que la clave pública debe usarse para encriptar mensajes dirigidos al propietario de la clave privada y para verificar su firma.

5.2. LA FIRMA ELECTRÓNICA.

Entendemos que se desprenden dos aspectos relativos a la firma electrónica, uno técnico y otro jurídico.

a) En efecto, desde un punto de vista técnico, la firma electrónica, a la luz del texto legal, es el resultado de un procedimiento informático fundado en el uso de un par

asociado de claves, una pública y otra privada, cuya nota esencial es que son distintas o asimétricas.

b) Desde un punto de vista estrictamente jurídico, la función de la firma electrónica es la verificación, es decir, la prueba del autor y de la integridad del contenido del documento.

En este sentido, la firma electrónica, de acuerdo con el texto legal, cumple una función igual que la suscripción tradicional del documento en formato papel.

La firma electrónica o digital es un código informático que permite determinar la autenticidad de un documento electrónico y su integridad, impidiendo a su transmisor desconocer la autoría del mensaje en forma posterior. Resulta de un proceso informático validado, implementado a través de un sistema criptográfico de claves públicas y privadas.[102]

5.2.1. FIRMA ELECTRÓNICA AVANZADA.

Es la firma electrónica que permite la identificación del firmante y ha sido creada por medios que este puede mantener bajo su exclusivo control, de manera que esta vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier modificación anterior de estos.[103]

---

[102] Secretaría de la Función Pública. Infraestructura de la Firma Digital. (www.pki.gov.ar)

[103] www.delitosinformaticos.com/seguridad/firma.shtml

Ahora bien, el firmante, es la persona que cuenta con un dispositivo de creación de firma y que actúa en nombre propio o en el de una persona física o jurídica a la que representa.

Una firma electrónica es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje. La firma electrónica es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos electrónicos, posibilitando que éstos gocen de una característica que únicamente era propia de los documentos en papel. Es un instrumento con características técnicas y normativas. Esto significa que existen procedimientos técnicos que permiten la creación y verificación de firmas electrónicas, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen. Sin embargo, no implica asegurar la confidencialidad del mensaje; un documento firmado electrónicamente puede ser visualizado por otras personas, al igual que cuando se firma holográficamente.

Con todo lo expuesto se entiende por "Firma Electrónica", la Información que, creada o utilizada por el signatario y asociada al mensaje de datos, permite atribuirle su autoría bajo el contexto en el cual ha sido empleado.

El beneficio de la firma digital sería facilitar la autenticación a distancia, constituyendo el mecanismo esencial para proveer seguridad y desarrollar la confianza entre partes mediante las redes abiertas. Para que un documento tenga validez jurídica, las firmas digitales deben permitir verificar tanto la identidad del

autor, como comprobar que dichos datos no han sufrido alteración desde que fueron firmados. Por ello constituye un elemento clave para el desarrollo del comercio electrónico en Internet.

a. Firma electrónica; que autentifica la identidad de la persona, es como mostrar nuestra cédula de identidad para que se confirme quien soy.
b. Firma electrónica Avanzada; autentifica la identidad pero además permite llevar a cabo transacciones comerciales avanzadas y contratos, es como ir a la notaria donde muestro mi cédula de identificación pero además se confirma ante el notario la legalidad de la transacción o relación.[104]

En la Ley Modelo de Firma Digital, en el Titulo III, Firma electrónica, certificados electrónicos y entidad acreditadora, Capitulo I, Firma electrónica, señala:

Artículo 33 (Requisitos esenciales de la firma electrónica)
El uso de la firma electrónica deberá cumplir con los siguientes requisitos:

a) Que vincule exclusivamente el mensaje de datos o documento a su titular;
b) Que permita verificar inequívocamente la autoría e identidad del signatario;
c) Que el dispositivo de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual fue generado y/o comunicado;
d) Que los datos de creación de la firma estén, al momento de la firma bajo el control exclusivo del signatario;

[104] Clasificación según la Ley Modelo de Firma Digital.

e) Que permita detectar cualquier alteración de esa información hecha después del momento de la firma.

Articulo 34. (Efectos)

La firma electrónica tendrá la misma fuerza, validez y efectos jurídicos que la ley otorga a la firma manuscrita, cuando ésta cumpla con los requisitos establecidos en el artículo 33 y se encuentre respaldada por un certificado electrónico vigente.

5.2.2. CERTIFICACIÓN DE FIRMA ELECTRÓNICA.

Es imperiosa la necesidad de que exista una Autoridad Certificante de claves públicas que certifique la correspondencia entre una clave pública y la persona física o jurídica titular de la misma, mediante la emisión de un certificado de clave pública. Este permitirá identificar inequívocamente al firmante del documento digital, evitando así la posibilidad del posterior repudio.

Los certificados digitales son pequeños documentos digitales que dan fe de la vinculación entre una clave pública y un individuo o entidad.[105] De este modo, permiten verificar que una clave pública específica pertenece, efectivamente, a un

[105] El compromiso más SEGURO, FLEXIBLE y EFICAZ para la Protección de Datos y Seguridad de la Información. Global Risk, SL - Detectives -. - http://www.globalrisk.es

individuo determinado. Los certificados ayudan a prevenir que alguien utilice una clave para hacerse pasar por otra persona.

Es decir; es un documento electrónico emitido por el notario de fe pública, que acredita la correspondencia entre una clave pública y la persona que es titular de la misma. El Certificado Electrónico se define como aquel mensaje de datos, que al ser proporcionado por un Proveedor de Servicios de Certificación, le otorga validez y certeza a la Firma Electrónica. Como aquel documento electrónico generado y firmado digitalmente por una entidad de certificación que vincula un par de claves con una persona determinada confirmando su identidad.

En su forma más simple, el certificado puede contener una clave pública y un nombre. Habitualmente, también contiene una fecha de expiración, el nombre de la Autoridad Certificante que la emitió, un número de serie y alguna otra información. Pero lo más importante es que el certificado propiamente dicho está firmado digitalmente por el emisor del mismo.

Dichas entidades intervienen como Terceros de confianza en las relaciones que las partes pueden llevar a cabo por medios electrónicos.

En Ley Modelo de Firma Electrónica, en el Articulo 37. Señala: (Requisitos de los certificados electrónicos)

I. Los requisitos de los certificados electrónicos emitidos o generados para respaldar la identidad del signatario y permitirle crear su par de claves, deberán contener:

a) El código identificativo único del certificado;
b) La identidad y domicilio de la Entidad de Certificación que expide el certificado**;**
c) La firma electrónica de la Entidad de Certificación Acreditada o la entidad pública que expide el certificado;
d) La identificación del signatario, en el supuesto de personas naturales, por su nombre y apellidos y su número de cédula de identidad o a través de un seudónimo, que existe como tal de manera inequívoca;
e) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del signatario
f) El comienzo y el fin del período de validez del certificado.

II. A los certificados electrónicos emitidos con un fin especifico, se les deberá incorporar el propósito con el que se generan.

Artículo 51 (Seguridad, integridad y disponibilidad de la información)

Todo repositorio deberá garantizar la seguridad, integridad y disponibilidad de la información en el contenido, la que deberá ser respaldada con copias de seguridad y bajo las siguientes características:

a) Estar respaldada con cada proceso de actualización de documentos;
b) Mantener una copia de seguridad en el lugar de operaciones de los sistemas de información y otra en el centro de almacenamiento de datos, propio o provisto por terceros.
c) El esquema de respaldo deberá ser simple y basado en la generación de copias acumulativas, con el objeto de mantener la historia de la información en el mínimo de versiones posibles.

5.3. CONTROL DE ACCESOS.

Es importante contar con llaves de acceso por que podríamos guardar en sistema documentación importante o simplemente hacer una transacción mediante medios telemáticos.

En la mayoría de los sistemas existen diferentes llaves de acceso. Estas nos permiten entrar a un sistema y de su seguridad depende que nadie más que los autorizados tengan acceso al sistema.

Las primeras llaves de acceso de las que hablaremos son los PINs (Personal Identification Number)[106], estos son muy usados por ejemplo en un ATM (Automatic Teller Machine) o cajero automático, en las cajas de seguridad de un hotel, en el control de acceso de una puerta electrónica, etc.

Otro tipo de llaves de acceso son los "Passwords", un password es usado principalmente en cuentas de e-mails, o acceso a una PC. Un password debe de garantizar la seguridad de acceso a un sistema.[107]

Un password debe ser aprendido y recordado cuando es usado, por lo que en la práctica son más usados passwords fáciles de recordar. No existe un método que sea el mas adecuado, sin embargo la misma practica sugiere uno como el siguiente: en lugar de una palabra fácil de recordar se puede elegir una frase larga pero fácil de recordar, por ejemplo, "Entre los individuos como entre las naciones el respeto al derecho ajeno es la paz", luego entonces se construye la password tomando la primera letra de la primera palabra y después la segunda de la segunda, la primera de la tercera, la segunda de la cuarta y así sucesivamente, entonces nuestro password queda como "eoioeanlrldjeap".

---

[106] CANO, J. (2004) Hacia un concepto extendido de la mente segura. Pensamiento sistémico en seguridad informática. Artículo de investigación (En revisión). Universidad de los Andes

[107] * CANO, J. (2000) *Programación Segura? Conceptos y Aspectos Técnicos*. Conferencia Magistral. Congreso Nacional de Estudiantes de Ingeniería de Sistemas. Santafe de Bogotá. Colombia. Universidad Distrital.

Finalmente otro tipo de llaves de acceso son las conocidas últimamente como claves criptográficas simétricas, este tipo de llaves son usadas para establecer una conexión segura a través de un canal inseguro como Internet o cualquier otro medio de comunicación insegura.

5.4. AUTENTICACIÓN Y CONTROL.

Los algoritmos criptográficos representan, directa o indirectamente, el único procedimiento conocido para garantizar la confidencialidad y la autenticidad de los documentos electrónicos, mediante la clave secreta, la firma electrónica y las autoridades de certificación.

5.5. NOTARIOS ELECTRÓNICOS.

Se ha de tender, por consiguiente, a dotar a estos documentos electrónicos de la necesaria seguridad, autenticidad, integridad y veracidad, proporcionándoles, además, la suficiente confidencialidad, a fin de asegurar que el contenido del documento no sea accesible a extraños a la relación contractual establecida. Esto es posible a través de las firmas electrónicas, que no son más que unas claves criptográficas asimétricas en las que se combinan claves, pública y privada, como tantas veces habíamos mencionado, que encriptan el documento impidiendo su manipulación y su público conocimiento, dando constancia de la autoría de las declaraciones de voluntad contenida en el mismo. Además de ello, se puede reforzar esta autenticación mediante la intervención de un tercero que actúe como fedatario electrónico, certificando que el firmante es quien dice ser, que esa firma

le corresponde y que con ella asume las obligaciones derivadas del contrato, las cuales quedan indisolublemente unidas a la firma digital utilizada en el documento.

Las nuevas tecnologías de Información y comunicación han transformado con su aplicación, casi todas las actividades que el ser humano realiza en el umbral de este siglo XXI. Visto de esta manera, el Derecho y específicamente la actividad notarial, se insertan paulatinamente en el moderno esquema de sociedad digital, para dar paso a una nueva generación de actividades y procesos sistematizados, cada vez más lejos del papel, elemento fundamental en la certificación de documentos de orden legal. El papel ha sido hasta hoy el sustrato básico del oficio notarial.

En términos simples, el notario es el licenciado en Derecho a quien el Estado concede el poder de dar fe pública y que tiene a su cargo por oficio: recibir, interpretar, redactar y dar forma legal y certeza jurídica a la voluntad de las personas que ante él acuden para otorgar actos jurídicos o para hacer constar hechos jurídicos, mediante su consignación en instrumentos públicos auténticos, es decir, con valor de prueba plena.[108]

5.6. FUNCIONES DE LOS NOTARIOS ELECTRÓNICOS.

[108] Lic. Francisco Xavier Arredondo Galván. Notario Público 173 . Febrero, 2003. arredondo@notaria173.com

El notario cumple una de las más importantes finalidades del Derecho, que es brindar seguridad jurídica, a través del ejercicio de varias funciones, entre las que destacan las siguientes:[109]

d) **Asesora**: Ofrece su consejo jurídico a cualquier persona, institución o empresa que lo requiera, dentro de un marco legal de servicio obligatorio institucional a los ciudadanos.

e) **Interpreta la voluntad**: Recibe e interpreta la voluntad de las personas que acuden ante él para la obtención de un servicio notarial concreto.

f) **Da forma, legaliza y legitima**: Cumple con la formalidad exigida por el Código Civil para ciertos actos jurídicos, es decir, dota de plena validez jurídica, a ciertos actos jurídicos que deben otorgarse de manera obligatoria ante su fe, como la compraventa de inmuebles, el condominio, el testamento, etc., y confiere, además, al documento público que produce, la garantía de legalidad absoluta.

g) **Tiene el poder de la fe pública**: Confiere autenticidad y certeza jurídica a ciertos hechos y actos jurídicos, mediante la consignación de ellos en el protocolo, dotándolos así de valor de prueba plena ante las autoridades y la sociedad.

---

[109] -Derecho gratis - Consultas e información sobre legislación y jurisprudencia

h) **Crea documentos auténticos**: Es autor responsable de los instrumentos públicos notariales que circulan con valor de prueba plena ante la comunidad nacional e internacional. Además, conserva los instrumentos originales otorgados y autorizados en el protocolo y expide un primer testimonio auténtico con fuerza ejecutiva a solicitud de los interesados y reproduce ilimitadamente nuevas copias auténticas.

Debería existir Acceso de seguridad, es decir, la micro forma (imagen reducida de un documento grabado en material idóneo para ser presentado como prueba y su contenido deberán darse fe de los mismos por un fedatario por un notario público para su validez como prueba, para lo cual estos deberán presentar su "Diploma de seguridad y capacidad técnica" para su certificación.

La función notarial no es ni será obsoleta, lo que parece empezar a serlo es la manera de prestar el servicio notarial con base en el tradicional documento, únicamente en soporte papel. Lo que el notario requiere hoy, es adaptarse a las exigencias y transformaciones del mundo actual e incorporar en su quehacer herramientas como la informática, la criptografía y la telemática.

CAPITULO VI

MARCO JURÍDICO

Se establece un marco jurídico en nuestro país con respecto a la Informática en general, sin embargo no existe una legislación específica que proteja a los documentos electrónicos como medio probatorio, por lo que se aplica la legislación

general vigente. Puesto que se corre el riesgo de que dichos documentos sean alterados, modificados, falsificados o destruidos por el fácil acceso de las personas a los sistemas informáticos.

En un escenario en el que claramente estamos asistiendo al fin de la primacía de la civilización del papel y en el que la revolución tecnológica ha llegado a todas las esferas del quehacer nacional, urge contar con una legislación adecuada que permita dotar al sistema de las garantías de seguridad y certeza jurídica necesarias destinadas a generar un marco de confianza para las personas.

6.1. LEGISLACIÓN BOLIVIANA.

En Bolivia, en el año de 1989, se consideró el análisis y tratamiento sobre Legislación Informática concerniente a contratación de bienes y servicios informáticos, flujo de información computarizada, modernización del aparato productivo nacional mediante la investigación científico- tecnológica en el país y la incorporación de nuevos delitos emergentes del uso y abuso de la informática.

Este conjunto de acciones tendientes a desarrollar de manera integral la informática, se tradujo en el trabajo de especialistas y sectores involucrados, representantes en el campo industrial, profesionales abogados y especialistas informáticos, iniciándose la elaboración del Proyecto de Ley Nacional de Informática, concluido en febrero de 1991.

Asimismo, el Código Penal Boliviano, texto ordenado según ley No 1768 de 1997, incorpora en el Título X un capítulo destinado a los Delitos Informáticos. Ambos cuerpos legales tratan de manera general los nuevos delitos emergentes del uso de la informática.

La Ley No 1768, no obstante de no estar exenta de la problemática actual, al abordar en el Capítulo XI la tipificación y penalización de delitos informáticos, no contempla la descripción de estas conductas delictivas detalladas anteriormente.

Articulo 363 bis (MANIPULACIÓN INFORMÁTICA). - El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días.

Articulo 363 ter (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS).- El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa

hasta doscientos días.[110]

Por consiguiente, la atipicidad de las mismas en nuestro ordenamiento jurídico penal vigente imposibilita una calificación jurídico-legal que individualice a la mismas, llegando a existir una alta cifra de criminalidad e impunidad, haciéndose imposible sancionar como delitos, hechos no descriptos en la legislación penal con motivo de una extensión extralegal del ilícito penal ya que se estaría violando el principio de legalidad expreso en la máxima "Nullum crime sine lege" Así mismo resulta imposible extender el concepto de bienes muebles e inmuebles a bienes incorporales como ser los datos, programas e información computarizada.

Respecto a los medios de prueba, el Código de Procedimiento Penal dice:

Articulo Nº 216.- (Documentos).- Se admitirá toda prueba documental ilícitamente obtenida.

El imputado no podrá ser obligado a reconocer documentos privados que obren en su contra, debiendo el juez o tribunal interrogarle se esta dispuesto a declarar sobre su autenticidad, sin que su negativa le perjudique. En este caso, las partes podrán acreditar la autenticidad por otros medios.

Articulo Nº 217.- (Documentos y elementos de convicción).- Los documentos, objetos y otros elementos de convicción incorporados al proceso podrán ser exhibidos al imputado, a los testigos y a los peritos para que los reconozcan e informen sobre ellos. Los que tengan carácter reservado, serán examinados

[110] Código Penal. Titulo XII, delitos contra la propiedad. Capitulo XI, delitos informáticos. Pag. 107 y 108.

privadamente por el juez o tribunal y si son útiles para la averiguación de la verdad, los incorporaran al proceso.[111]

Código De Procedimiento Civil. Prueba. [112]Articulo Nº 374.- (Medios legales de Prueba) Son medios legales de prueba:

1. Los documentos.
2. La confesión.
3. La inspección judicial.
4. El peritaje.
5. La testificación.
6. La presunción. .

Forma y prueba. Para evitar confusiones, recordemos que la forma constituye un elemento esencial del acto jurídico, en la medida que es el modo en que el sujeto se relaciona con el objeto, valer decir forma es la exteriorización de la voluntad del sujeto en relación a la consecución del fin jurídico propuesto, es lo que hace visible la manifestación de voluntad.

En ciertos casos la forma, debe cumplir requisitos establecidos por la ley, para que el acto tenga validez. Es la llamada forma legal (ejemplo: la escritura pública, forma esencial o solemne para la transmisión de derechos reales sobre cosas inmuebles (Art. 1287 C.Civ).

---

[111] Nuevo Código de Procedimiento Penal. Titulo V, documentos y otros medios de prueba. Pág. 165 y 166.

[112] Código de Procedimiento Civil. Capitulo VI, prueba. Pág. 111.

En el Decreto Supremo 27328, en la Sección IV, sobre Contrataciones Electrónicas, señala lo siguiente:

Articulo 34.- (Contratación por medios electrónicos). La contratación de bienes y servicios podrá realizarse por medios electrónicos, en el marco de la reglamentación especial, que regulara el uso de medios electrónicos y reconocerá la validez del mensaje de datos, documento electrónico, firma electrónica y transacciones electrónicas para garantizar la transparencia, autenticidad y confidencialidad.

Bajo este régimen podrán ser contratados los bienes y servicios que por sus características de uniformidad, homogeneidad e identidad sean de tipo estándar, estén disponibles en el mercado y se encuentren registrados en el Catalogo de Bienes vigente.

La adjudicación bajo esta forma de contratación se efectuara por el método de precio mas bajo o subasta a la baja, de acuerdo con los procedimientos de contratación establecidos en la reglamentación especial.

La contratación por medios electrónicos será implementada gradualmente, debiendo el Órgano Rector desarrollar un adecuado proceso de difusión, capacitación y asistencia técnica, promoviendo la adaptación de las entidades públicas.

El hecho de estar legislado el sistema de contratación electrónica, provee la necesaria seguridad jurídica a los documentos electrónicos a propósito de las licitaciones y propuestas electrónicas.

Ahora mencionaré algunos artículos del Proyecto de Ley de Documentos, Firmas y Comercio Electrónico. En el Titulo II, Documentos y contratación electrónica:

Artículo 7.- (Reconocimiento jurídico).

I. En razón a su naturaleza jurídica, los documentos electrónicos podrán ser los siguientes:

   a) Documentos públicos firmados electrónicamente por personas que legalmente cuenten con la atribución y la facultad de dar fe pública, judicial, registral, notarial o administrativa, siempre y cuando actúen en el ámbito de sus competencias y de acuerdo a los requisitos exigidos por ley;
   b) Documentos expedidos y firmados electrónicamente por funcionarios públicos en el ejercicio de sus funciones, de conformidad a la legislación específica;
   c) Documentos privados;
   d) Documentos tributarios de acuerdo a la normativa especifica.

II. No se negará efectos y validez jurídica y/o probatoria, a la información contenida en documentos por la sola razón de estar en forma electrónica, sea

que la información se encuentre encriptada y/o cifrada, y respaldada por un certificado electrónico.

III. Los documentos electrónicos tendrán igual valor jurídico que los documentos escritos, siempre que se encuentren suscritos con la firma electrónica. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y sus reglamentos.

IV. La factura electrónica, la declaración jurada y otros documentos que no precisen de certificación expresa conforme a normativa tributaria tendrán pleno valor probatorio.

Artículo 8.- (Celebración por escrito).

En todos los casos en que se exija que una información conste por escrito o deba ser presentada de esa forma, o bien se prevea la existencia de consecuencias jurídicas para el evento de que la información no conste por escrito, se entenderá que un documento electrónico cumple con el requisito de escritura pública, cuando la información contenida en el mismo sea legible, esté íntegra, sea susceptible de ser archivada y recuperada en cualquier momento y sea posible la verificación del remitente o de su creador.

Artículo 11. (Conservación de documentos)

Cuando la ley requiera que los documentos, registros o informaciones sean almacenados, ese requisito se considerará satisfecho mediante la conservación del documento electrónico en un repositorio siempre que reúnan las siguientes condiciones:

a) Que la información que contenga el documento sea accesible para su posterior consulta.
b) Que sea conservado con el formato en que se hubiera generado, enviado o recibido o con algún formato que demuestre la reproducción exacta de la información generada, enviada o recibida.
c) Que se conserve todo dato que permita determinar el origen, el destino del documento electrónico, la fecha y hora en que fue creado, generado, procesado, enviado, recibido y archivado.
d) Que se garantice la integridad del documento electrónico almacenado.

En el Capitulo II, Documentos públicos. Artículo 15 (Documentos públicos electrónicos).

I. Se reconoce la validez y eficacia jurídica de los documentos electrónicos otorgados, conferidos, autenticados y autorizados, expedidos por ante Notario de fe Pública y firmado por el o los comparecientes mediante una firma electrónica.

II. Dichos instrumentos públicos electrónicos deberán observar por analogía y en todo lo que fuere aplicable, los requisitos, formalidades y solemnidades exigidas por la Ley y demás normas pertinentes.

Artículo 16 (Otorgación de escritura pública).

Cuando para efectos legales se exija la existencia o el otorgamiento de una escritura pública, o bien se prevea consecuencias jurídicas para el evento de que falta dicha solemnidad, se entenderá que un documento electrónico cumple con esa exigencia si satisface las siguientes condiciones:

a) Que el Notario de fe Pública de fe del acto jurídico, mediante los medios establecidos en la presente Ley y sus reglamentos;
b) Que se haya utilizado un procedimiento que permita identificar a los comparecientes en el documento electrónico, para indicar que su contenido cuenta con la aprobación de aquellas, y que permita que las partes lo firmen electrónicamente y un Notario de fe Pública autorizará mediante una firma electrónica;
c) Que el método o procedimiento utilizado cumpla los requisitos exigidos por la Ley del Notariado, Código Civil y disposiciones aplicables, según la naturaleza del contrato.

En el Capitulo V, Reglas Probatorias. El artículo 31 (Admisión y valoración).

I. Constituyen prueba los mensajes de datos, documentos electrónicos, contratos electrónicos, firmas electrónicas y certificados electrónicos u otro contenido en medios electrónicos que cumplan los requisitos establecidos en la presente Ley.

II. Para la admisión, valoración y efectos legales se observará lo dispuesto en la presente Ley, el Código Civil, Código de Comercio, Código de Procedimiento Civil, Ley de Procedimientos Administrativos y demás normas aplicables.

Artículo 32. (Fuerza Probatoria).

En función de los principios establecidos en la presente Ley, para otorgar fuerza probatoria a los mensajes de datos, documentos electrónicos, contratos electrónicos, firmas electrónicas, certificados electrónicos u otros contenidos en medios electrónicos, se deberá considerar lo siguiente:

a) La fiabilidad de la forma en la que se haya generado;
b) La fiabilidad de la forma en la que se haya archivado, comunicado el mensaje o emitido por Entidad de Certificación;
c) La fiabilidad de la forma en la que se haya conservado la integridad y la autenticidad de la información; y
d) La forma en la que se identifique a su iniciador y cualquier otro factor pertinente que sea establecido en la presente Ley y sus reglamentos.

Artículo 63. (Confidencialidad en el comercio electrónico).

Se prohíbe cualquier forma de interceptación o vigilancia de las comunicaciones relacionadas con el comercio electrónico, que no sea su remitente o su destinatario, salvo que esté legal y/o judicialmente autorizado para ello.

En el Titulo V, Delitos informáticos. Articulo 72.- (Modificaciones al Código Penal).

9. Inclúyase como artículo 363 quater del Código Penal, el siguiente:

“Art. 363.- (FALSIFICACIÓN Y SUPLANTACIÓN DE IDENTIDAD ELECTRÓNICA).

I. Será sancionado con reclusión de uno a seis años, el que causando perjuicio ajeno u obteniendo ventaja para sí o un tercero, para el caso de documentos públicos:
   a) Simule o altere un mensaje de datos en todo o en parte, utilizando los datos personales, la identidad física o electrónicos electrónica que no le pertenecen;
   b) Altere el contenido de un mensaje de datos en algunos de sus elementos o etapas de transmisión;
   c) Intercepte, interfiera y/o altere el proceso mismo de transmisión del mensaje de datos entre los titulares de origen y destino del mismo.

II. En el caso de documentos privados, la falsificación y suplantación de identidad electrónica, será sancionada con una pena privativa de libertad de dos a seis años”.

10. Inclúyase como artículo 363 quinquies del Código Penal, el siguiente:

“(SABOTAJE INFORMÁTICO). Quien obstaculice, modifique o atentare contra el normal funcionamiento de un sistema de información, impidiendo la ejecución de sus funciones, o ralentizando los mismos, mediante recursos físicos o lógicos; incurrirá en privación de libertad de uno a tres años”.

11. Inclúyase como artículo 363 sexties del Código Penal, el siguiente:

“(OBTENCIÓN Y UTILIZACIÓN NO AUTORIZADA DE INFORMACIÓN). La persona o personas que obtuvieren información sobre datos personales o institucionales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, será sancionado con reclusión de seis meses a dos años”.

En el Texto Ordenado de la Ley No 1488 de Bancos y Entidades Financieras. (al 5 de mayo de 2004), en el Titulo primero , Capitulo I, Ámbito de la Ley.

Nota: articulo modificado por el articulo 6º de la Ley No 2297 de 20 de diciembre de 2001.

Artículo 3.- Son actividades de intermediación financiera y de servicios auxiliares del sistema financiero, las siguientes:

1.- Recibir dinero de personas naturales o jurídicas como depósitos, prestamos o mutuos, o bajo otra modalidad para su colación conjunta con el capital de la entidad financiera, en créditos o en inversiones del propio giro.

2.- Emitir, descontar o negociar valores y otros documentos representativos de obligaciones.

3.- Prestar servicios de depósitos en almacenes generales de depósito, si esta actividad la efectúa la filial de un banco.

4.- Emitir cheques de viajero y tarjetas de crédito.

5.- Operar y administrar buros de información crediticia, cuando esta actividad la realice una sociedad anónima de giro exclusivo.

6.- Efectuar fideicomisos y mandatos de intermediación financiera, administrar fondos de terceros; operar cámaras de compensación y prestar caución y fianza bancaria.

7.- Realizar operaciones de arrendamiento financiero y factoraje.

8.- Valuar las entidades del sistema financiero.

Las operaciones efectuadas en el marco de las actividades mencionadas en el presente artículo podrán realizarse a través de medios electrónicos. Estas operaciones y la información contenida y transmitida como mensajes electrónicos de datos tendrán los mismos efectos legales, judiciales y de validez probatoria que un documento escrito con firma autógrafa. La Superintendencia emitirá la

normativa de seguridad para las operaciones y transmisiones electrónicas efectuadas por las entidades de intermediación financiera.

En el marco del sistema de pagos, el Banco Central de Bolivia establecerá el marco normativo de la firma digital para otorgar seguridad y operatividad a las transferencias electrónicas.

6.2. DERECHO COMPARADO-NORMATIVA INTERNACIONAL.

Dado lo anterior a continuación se mencionan algunos aspectos relacionados con la ley en los diferentes países, así como con los delitos informáticos que persigue.

*PAÍSES.

En el contexto internacional, son pocos los países que cuentan con una legislación apropiada. Entre ellos, se destacan, Alemania, Austria, Gran Bretaña, Holanda, Francia, España, Estados Unidos, México, Chile, Argentina y Venezuela. [113]

6.2.1. ALEMANIA.

Este país sancionó en 1986 la Ley contra la Criminalidad Económica, que contempla los siguientes delitos:

---

[113] -Derecho gratis - Consultas e información sobre legislación y jurisprudencia.

* Espionaje de datos.

* Estafa informática.

* Alteración de datos.

* Sabotaje informático.

6.2.2. AUSTRIA.

La Ley de reforma del Código Penal, sancionada el 22 de Diciembre de 1987, sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes comenten este hecho utilizando su profesión de especialistas en sistemas.[114]

6.2.3. GRAN BRETAÑA.

Debido a un caso de hacking en 1991, comenzó a regir en este país la Computer Misuse Act (Ley de Abusos Informáticos). Mediante esta ley el intento, exitoso o no, de alterar datos informáticos es penado con hasta cinco años de prisión o multas. Esta ley tiene un apartado que específica la modificación de datos sin autorización.

6.2.4. HOLANDA.

[114] Derecho gratis - Consultas e información sobre legislación y jurisprudencia.

El 1º de Marzo de 1993 entró en vigencia la Ley de Delitos Informáticos, en la cual se penaliza los siguientes delitos:

* El hacking.

* El preacking (utilización de servicios de telecomunicaciones evitando el pago total o parcial de dicho servicio).

* La ingeniería social (arte de convencer a la gente de entregar información que en circunstancias normales no entregaría).

* La distribución de virus.

6.2.5. FRANCIA.

Francia fue uno de los primeros países en generar cambios en esta materia. En efecto, el 12 de julio de 1980 se promulgó la ley 80/525, donde se establece que "Los documentos emitidos, cualquiera sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación".[115]

[115] -El Boga - Leyes, agrupaciones, organizaciones, constituciones internacionales y otros recursos.

Además de la norma ya citada, encontramos mención a los medios electrónicos en la Ley 78-17, del 6 de enero de 1978, relativa a la Informática, los Archivos y las Libertades. Existen dos Capítulos, el Capítulo III, titulado "De los trámites previos a la puesta en práctica de tratamientos automatizados", y el Capítulo IV, llamado "De la colecta, registro y conservación de informaciones nominativas"; en donde se menciona el uso de estos medios.

En enero de 1988, este país dictó la Ley relativa al fraude informático, en la que se consideran aspectos como:

* Intromisión fraudulenta que suprima o modifique datos.
* Conducta intencional en la violación de derechos a terceros que haya impedido o alterado el funcionamiento de un sistema de procesamiento automatizado de datos.
* Conducta intencional en la violación de derechos a terceros, en forma directa o indirecta, en la introducción de datos en un sistema de procesamiento automatizado o la supresión o modificación de los datos que éste contiene, o sus modos de procesamiento o de transmisión.
* Supresión o modificación de datos contenidos en el sistema, o bien en la alteración del funcionamiento del sistema (sabotaje).

6.2.6. ESPAÑA.

"Los documentos emitidos, cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o los que éstas emitan como copias de originales almacenados por estos mismos medios gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por leyes."[116]

El documento electrónico es admisible en los países de sistema de libre apreciación de la prueba, conforme a las reglas de la sana crítica para aquellos medios de prueba no excluidos en forma expresa en la ley, en este sentido, el juzgador le deberá atribuir los efectos y fuerza probatoria después de una adecuada valoración y comprobación de autenticidad.

En el Nuevo Código Penal de España, se establece que al que causare daños en propiedad ajena, se le aplicará pena de prisión o multa. En lo referente a:

* La realización por cualquier medio de destrucción, alteración, inutilización o cualquier otro daño en los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.
* El nuevo Código Penal de España sanciona en forma detallada esta categoría

[116] -El Boga - Leyes, agrupaciones, organizaciones, constituciones internacionales y otros recursos.

delictual (Violación de secretos/Espionaje/Divulgación), aplicando pena de prisión y multa.

* En materia de estafas electrónicas, el nuevo Código Penal de España, solo tipifica las estafas con ánimo de lucro valiéndose de alguna manipulación informática, sin detallar las penas a aplicar en el caso de la comisión del delito.

Partiendo de la Norma Constitucional, el legislador español ha dictado normas que limitan el uso de la Informática, esto, en función de garantizar el respeto al honor y a la intimidad personal. Estos principios, preceptuados en el. Artículo 18.4 de la Carta Magna Española, son luego desarrollados en la ley 5/1998, de 6 de marzo, sobre "Protección Jurídica de la Base de Datos".

En materia Fiscal y Económico – Administrativa, es destacable el Artículo 88.2 de la Ley 37/1992, que regula el Impuesto sobre el Valor Añadido, en donde se admite la facturación electrónica.

La legislación española no solo reconoce y promueve el uso de los medios electrónicos, sino que además, considera al soporte magnético que contiene información, equivalente al documento tradicional, dándole el adjetivo de electrónico. A este respecto, podemos citar algunas disposiciones:

Artículo 45 de la Ley 30/1992 sobre el Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común:

> "Los documentos emitidos cualquiera que sea su soporte, por medios electrónicos, informáticos o telemáticos por las Administraciones Públicas, o

los que éstas emitan como copia de los originales almacenados por estos mismos medios, gozarán de la validez y eficacia del documento original, siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de las garantías y requisitos exigidos por ésta u otras leyes".[117]

Artículo 76.3.c.2 del Reglamento del Impuesto sobre Transmisiones Patrimoniales y Actos Jurídicos documentados: "…cualquier soporte escrito, incluidos los informáticos, por los que se pruebe, acredite o se haga constar alguna cosa" (Definición de Documento, según ese Reglamento).

Artículo 26 de la Ley 10/1995, de 26 de noviembre, del Código Penal: "A los efectos de este Código se considera documento todo soporte material que exprese o incorpore datos, hechos o narraciones con eficacia probatoria o cualquier otro tipo de relevancia jurídica".

Es importante resaltar, además, el Artículo 230 de la Ley Orgánica del Poder Judicial, en donde se admite el documento electrónico, dándole validez y eficacia; así como todas las normas anteriormente citadas.

---

[117] -El Boga - Leyes, agrupaciones, organizaciones, constituciones internacionales y otros recursos.

6.2.7. ESTADOS UNIDOS.

Este país adoptó en 1994 el Acta Federal de Abuso Computacional que modificó al Acta de Fraude y Abuso Computacional de 1986.

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas. La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

Asimismo, en materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, la legislación estadounidense sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

En el mes de Julio del año 2000, el Senado y la Cámara de Representantes de este país -tras un año largo de deliberaciones- establece el Acta de Firmas Electrónicas en el Comercio Global y Nacional. La ley sobre la firma digital responde a la necesidad de dar validez a documentos informáticos -mensajes electrónicos y contratos establecidos mediante Internet- entre empresas (para el B2B) y entre empresas y consumidores (para el B2C).

Otro proyecto de la Casa Blanca modifica las leyes que regulan la intimidad y la intervención de las telecomunicaciones (Privacy Act y Wiretap Act) para poder interceptar y desencriptar mensajes electrónicos enviados o recibidos por sospechosos o presuntos terroristas, con plena eficacia procesal como prueba documental incluso cuando dichas evidencias hayan sido obtenidas sin el correspondiente mandamiento judicial.

Este proyecto también prevé la asignación de una partida presupuestaria para que el Fiscal General pueda solicitar a compañías telefónicas, electrónicas y de seguridad informática el diseño de tecnologías de intervención de las telecomunicaciones.

Todo ello va acompañado de un intenso debate sobre las posibilidades de desencriptación y la posible vulneración del derecho a la intimidad.

6.2.8. MÉXICO.

El documento electrónico o informático, se concibe como un medio de expresión de la voluntad con efectos de creación, modificación o extinción de derechos y obligaciones por medio de la electrónica, informática y telemática.

Si analizamos la noción tradicional de documento referida al instrumento en el que queda plasmado un hecho que se exterioriza mediante signos materiales y permanentes del lenguaje, vemos como el documento electrónico cumple con los requisitos del documento en soporte de papel en el sentido de que contiene un mensaje (texto alfanumérico o diseño gráfico) en lenguaje convencional (el de los bits) sobre soporte (cinta o disco), destinado a durar en el tiempo.

El Artículo 289 del Código de Procedimientos Civiles señalaba expresamente los medios de prueba, pero actualmente, la redacción de este Artículo ha cambiado, al introducir la expresión de que "son admisibles como medios de prueba aquellos elementos que puedan producir convicción en el ánimo del juzgador acerca de los hechos controvertidos o dudosos".

Lo cierto es que, a pesar de la disposición ya citada, no existe disposición expresa que señale cual es el valor probatorio que podría atribuírsele a los medios electrónicos, salvo lo que dispone la Ley sobre Mercado de Valores. Siendo así, la situación reviste dificultades al tratar de aplicarlos in extenso, por lo que se hace necesario estudiar para su aplicación cada caso en particular.

6.2.9. VENEZUELA.

Venezuela es, el que más tarde incorpora en sus normas el uso de la Informática y de los medios electrónicos. En efecto, no es sino hasta 1999, con la Constitución

de la República Bolivariana de Venezuela que encontramos mención expresa acerca de la regulación del uso de la Informática. (Artículos 60 y 108).

Sin embargo, el uso de los medios electrónicos en tiempos anteriores no podría ser catalogado de ilícito o ilegal, puesto que es bien sabido que en Venezuela es aceptado el Sistema de libertad probatoria, tal y como lo señala el Artículo 395 del Código de Procedimiento Civil.

Además de la Norma Constitucional, que como ya dijimos regula el uso de la Informática, encontramos mención sobre el uso de los medios electrónicos en el Artículo 162, ordinal 3º del Código Orgánico Tributario, referido a la forma de practicar las notificaciones, cuando señala que estas pueden realizarse "…mediante correo público o privado, por sistemas de comunicación telegráficos, facsimilares, electrónicos y similares siempre que se deje constancia en el expediente de su recepción".[118]

A pesar de que, como fue indicado ya, existen desde 1999 normas que regulan el uso de la Informática, y que con el Vigente Código de Procedimiento Civil desde 1986 se reconoce el principio de libertad probatoria; no es sino hasta el 28 de febrero del 2001, con la puesta en vigencia del Decreto con Fuerza de Ley de

[118] -El Boga - Leyes, agrupaciones, organizaciones, constituciones internacionales y otros recursos.

Mensajes de Datos y Firmas Electrónicas, que se reconoce el valor probatorio de los medios electrónicos.

A este efecto, señala el Artículo 4º del mencionado Decreto, que los Mensajes de Datos gozarán de la misma eficacia probatoria que la ley le otorga a los documentos que constan en formato papel.

También es importante señalar que en aquellos casos en que la ley exija de la firma autógrafa para que un negocio jurídico surta efectos, quedará satisfecho al tener incorporada una firma electrónica. Por último, otro aspecto relevante que incorpora este Decreto es el principio de Neutralidad Tecnológica, mediante el cual no existe inclinación hacia una tecnología en particular, y que ha sido explicado previamente.

Por lo que respecta a la ley, ha sido paradójicamente, la Ley de Registro Público (en Venezuela), la que otorgó valor probatorio a los fotos tatos, extendiéndose posteriormente a todo tipo de reproducción mecánica o no (Art. 120 de la Ley de Registro Público, correspondiente al artículo 105 de las anteriores), posteriormente la reforma del Código de Procedimiento Civil, incluyó la prueba libre, con lo cual se despeja toda duda sobre su procedencia en juicio, estableciendo reglas para su valoración, pudiendo decirse, sin lugar a dudas, que tal reforma fue quién legalizó, definitivamente, la inclusión de todas estas pruebas reales, dentro del concepto de documento.

Dicho concepto es unívoco, y no puede hablarse de un documento civil, fiscal, penal etc., ya que el mismo, más que concepto jurídico, corresponde a la realidad de las cosas.

6.2.10. CHILE.

En Chile el documento electrónico es toda representación informática que da testimonio de un hecho.

Chile fue el primer país latinoamericano en sancionar una Ley contra delitos informáticos, la cual entró en vigencia el 7 de junio de 1993. Esta ley se refiere a los siguientes delitos:

* La destrucción o inutilización de los de los datos contenidos dentro de una computadora es castigada con penas de prisión. Asimismo, dentro de esas consideraciones se encuentran los virus.
* Conducta maliciosa tendiente a la destrucción o inutilización de un sistema de tratamiento de información o de sus partes componentes o que dicha conducta impida, obstaculice o modifique su funcionamiento.
* Conducta maliciosa que altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información.[119]

[119] -El Boga - Leyes, agrupaciones, organizaciones, constituciones internacionales y otros recursos.

El 12 de enero del 2002 se aprobó en Chile el Proyecto de Ley que regula el uso de la firma electrónica. En sus primeros artículos se indica el ámbito de aplicación de esta ley, el cual es el siguiente:

1. Los documentos electrónicos y sus efectos legales,
2. La utilización de la firma electrónica,
3. La prestación de servicios de certificación de firmas electrónicas, y
4. El procedimiento de acreditación al que deberán sujetarse los prestadores de servicio de certificación de firma electrónica avanzada.

También encontramos en sus primeros artículo los principios reguladores de la ley, siendo estos:

1. Libertad de prestación de servicios,
2. Libre competencia,
3. Neutralidad Tecnológica,
4. Compatibilidad Internacional, y
5. Equivalencia del soporte técnico al soporte papel.

A pesar de ser todos estos principios imprescindibles para el desarrollo de esta ley, son el tercero y el quinto de un valor característico. El principio de neutralidad tecnológica implica que esta ley mantiene su vigencia aún y cuando surjan nuevas tecnologías. Por ejemplo, cuando la ley, en su Artículo 2° define a la firma electrónica como "cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar a menos formalmente a su autor",

no está amarrando esta definición con algún método tecnológico en particular, sino que puede aplicarse a cualquier tecnología que en un futuro aparezca.

El principio de equivalencia del soporte técnico al soporte papel, o también llamado principio del equivalente funcional, está contenido en el Artículo 3 de esta ley. Este principio permite que todos aquellos actos jurídicos celebrados bien por personas naturales, bien por personas jurídicas, mediante el uso de medios electrónicos sean válidos y produzcan los mismos efectos que aquellos que constan en papel.

6.2.11. ARGENTINA.

La legislación argentina admite la presentación por vía electrónica de declaraciones de impuestos de las personas jurídicas (Ley 19.550) y de las personas físicas (Ley 23.314). La Ley 24.614 ordenó, en el ámbito de la Administración Pública Nacional, que:

> "Los documentos redactados en primera generación en soporte electrónico u óptico indeleble, y los reproducidos en soporte electrónico u óptico indeleble a partir de originales primera generación en cualquier otro soporte, serán considerados originales y poseerán, como consecuencia de ello, pleno valor probatorio, en los términos del Artículo 995 del Código Civil".[120]

---

[120] El Boga - Leyes, agrupaciones, organizaciones, constituciones internacionales y otros recursos.

Es decir, se les concede el valor de un instrumento público.

Los documentos electrónicos poseen valor probatorio, ya que según el Artículo 378 del Código Procesal Civil y Comercial de la Nación, el Juez puede admitirlos como medio probatorio. Así mismo, el Proyecto de Código Civil de 1998 contempla en sus Artículos 263 y 264 estos documentos, denominándolos instrumentos particulares.

Es importante señalar, que aunque no ha sido necesario la puesta en funcionamiento de la ley de firma digital para que ésta empiece a utilizarse, sí se requiere de la operatividad de la ley para que la firma digital adquiera validez probatoria.

Por último, encontramos una importante mención de los medios electrónicos y su valor probatorio en el Artículo 43 de la Ley de Procedimiento de Faltas de la Ciudad de Buenos Aires, cuando señala que:

"Las constancias obtenidas mediante el empleo de medios electrónicos, fílmicos, fotográficos o de grabación de videos, aprobados por la autoridad de aplicación que no sean enervadas por otra prueba de eficacia similar, pueden ser consideradas por el juez o jueza como suficiente prueba de la falta".[121]

[121] -El Boga - Leyes, agrupaciones, organizaciones, constituciones internacionales y otros recursos.

6.2.12. ECUADOR.

La legislación Ecuatoriana menciona que los mensajes de datos, firmas electrónicas, documentos electrónicos y los certificados electrónicos nacionales o extranjeros, serán considerados medios de prueba. A si mismo se da la presunción cuando como prueba se presentase una firma electrónica certificada por una realidad de certificación acreditada por consiguiente esta no ha sido alterado desde su emisión y que la firma pertenece a su signatario.

La Práctica de la prueba en este país se realiza observando las siguientes normas :

a. Al presentar un mensaje de datos en un proceso judicial se deberá adjuntar el soporte informático y la transcripción en papel del documento electrónico, así como los elementos necesarios, para su lectura y verificación.
b. En caso de impugnación del certificado o de la firma por cualquiera de las partes el Juez o Tribunal, a petición de parte ordenará a la entidad certificadora e información.
c. El facsímile, cuando haya sido enviado y recibido como mensaje de datos, que mantenga su integridad.

En caso que algunas de las partes niegue su validez, deberá probar que adolece de vicios ó que el procedimiento de seguridad y verificación no puedan ser reconocidos técnicamente severos.

Para la valoración de la prueba el juez deberá designar peritos.

6.3. ORGANIZACIONES.

La legislación extranjera o el "Derecho Comparado" existente en este ámbito es profusa, y de sobra conocidas son las normas sobre comercio electrónico y firmas electrónicas de los Grupos de Trabajo de la UNCITRAL, de las Directivas de la Unión Europea y de los EE.UU. Pero se trata de normas antiguas algunas (las de UNCITRAL), y de otras cuyos presupuestos son del todo ajenas a la realidad de Ibero América.

También es constatable como en Ibero América las normas locales (de países tales como Argentina, Colombia, Chile, Ecuador, Panamá, Perú, Venezuela, etcétera) han recogido el tenor de normas como las propuestas de UNCITRAL o la ley española sobre firma electrónica, olvidándose -por cierto- que los conceptos, las condiciones y los requisitos para asignar certeza técnica y jurídica en el uso de documentos electrónicos no son los mismos en América que en Europa, y que la América del Norte posee una realidad en materia de asignación de fe pública -que es lo que en esencia está en juego- anglosajona, muy distante de la connotación latina de nuestros países.

6.3.1. ORGANIZACIONES DE LAS NACIONES UNIDAS.

Finalmente es de destacar la actitud adoptada por las Naciones Unidas (a través de la UNCITRAL) quien, reconociendo las dificultades de que se llegue mediante la negociación a un acuerdo internacional sobre la materia, se ha decantado a

favor de una rápida adecuación de las legislaciones de cada país como medida de carácter más pragmático. Es de señalar que este organismo ha emitido un valioso documento, titulado Legal Value of Computer Records, en el que se expresa que las normas o reglas concernientes a las pruebas relativas a documentos electrónicos (si bien dice registros de computadora) no deben suponer un obstáculo para el uso de las tecnologías emergentes tanto a nivel doméstico como internacional.[122] Y señala que las normas redactadas por algunos países deben superar los problemas que genera el lenguaje empleado pues incorpora referencias culturales que todavía suponen un freno al desarrollo.

Pero el esfuerzo de los diferentes países no es suficiente ni tiene la velocidad con la que se está desarrollando este fenómeno en la práctica. Este término, velocidad, ha adquirido una importancia fundamental por cuanto implica, en temas de tecnología la adaptación al medio con ventaja sobre el resto.

Las Comisiones de Comunicaciones e Informática y de Legislación General, aconsejan la sanción del siguiente Proyecto de ley: Ley de firma digital. Considerado además como Ley Modelo de firma digital.

ARTICULO 2°.- Firma Digital. Se entiende por firma digital al resultado de aplicar a un documento digital un procedimiento matemático que requiere información de

---

[122] -El Boga - Leyes, agrupaciones, organizaciones, constituciones internacionales y otros recursos.

exclusivo conocimiento del firmante encontrándose esta bajo su absoluto control. La firma digital debe ser susceptible de verificación por terceras partes tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Los procedimientos de firma y verificación a ser utilizados para tales fines serán los determinados por la Autoridad de Aplicación en consonancia con estándares tecnológicos internacionales vigentes.

ARTICULO 5°.- Firma electrónica. Se entiende por firma electrónica al conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez.

ARTICULO 6°.- Documento digital. Se entiende por documento digital a la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento o archivo. Un documento digital también satisface el requerimiento de escritura.

ARTÍCULO 8°.- Presunción de integridad. Si el resultado de un procedimiento de verificación de una firma digital aplicado a un documento digital es verdadero, se presume, salvo prueba en contrario, que este documento digital no ha sido modificado desde el momento de su firma.

ARTICULO 11.- Original. Los documentos electrónicos firmados digitalmente y los reproducidos en formato digital firmados digitalmente a partir de originales de primera generación en cualquier otro soporte, también serán considerados originales y poseen, como consecuencia de ello, valor probatorio como tales, según los procedimientos que determine la reglamentación.

ARTÍCULO 12.- Conservación. La exigencia legal de conservar documentos, registros o datos, también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente, según los procedimientos que determine la reglamentación, siempre que sean accesibles para su posterior consulta y permita determinar fehacientemente el origen, destino, fecha y hora de su generación, envío y/ o recepción.

ARTÍCULO 13.- Certificado digital. Se entiende por certificado digital al documento digital firmado digitalmente por un certificador, que vincula los datos de verificación de firma a su titular.

ARTICULO 14.- Requisitos de validez de los certificados digitales. Los certificados digitales para ser válidos deben:

a) Ser emitidos por un certificador licenciado por el Ente Licenciante;

b) Responder a formatos estándares reconocidos internacionalmente fijados por la Autoridad de Aplicación y contener, como mínimo, los datos que permitan:

identificar indubitablemente a su titular y al certificador licenciado que lo emitió, indicando su período de vigencia y los datos que permitan su identificación única; ser susceptible de verificación respecto de su estado de revocación; diferenciar claramente la información verificada de la no verificada incluidas en el certificado; contemplar la información necesaria para la verificación de la firma; identificar la política de certificación bajo la cual fue emitido.

Y en Anexo, menciona algunos conceptos importantes, como ser:

INFORMACIÓN: conocimiento adquirido acerca de algo o alguien.

PROCEDIMIENTO DE VERIFICACIÓN**:** proceso utilizado para determinar la validez de una firma digital. Dicho proceso debe considerar al menos:

Que dicha firma digital ha sido creada durante el periodo de validez del certificado digital del firmante; que dicha firma digital ha sido creada utilizando los datos de creación de firma digital correspondientes a los datos de verificación de firma digital indicados en el certificado del firmante; la verificación de la autenticidad y la validez de los certificados involucrados.

DATOS DE CREACIÓN DE FIRMA DIGITAL: datos únicos, tales como códigos o claves criptográficas privadas, que el firmante utiliza para crear su firma digital.

DATOS DE VERIFICACIÓN DE FIRMA DIGITAL: datos únicos, tales como códigos o claves criptográficas públicas, que se utilizan para verificar la firma digital, la integridad del documento digital y la identidad del firmante.

DISPOSITIVO DE CREACIÓN DE FIRMA DIGITAL: dispositivo de hardware o software técnicamente confiable que permite firmar digitalmente.

DISPOSITIVO DE VERIFICACIÓN DE FIRMA DIGITAL: dispositivo de hardware o software técnicamente confiable que permite verificar la integridad del documento digital y la identidad del firmante.

POLÍTICAS DE CERTIFICACIÓN: reglas en las que se establecen los criterios de emisión y utilización de los certificados digitales.

TÉCNICAMENTE CONFIABLE: cualidad del conjunto de equipos de computación, software, protocolos de comunicación y de seguridad, y procedimientos administrativos relacionados, que cumpla los siguientes requisitos:

1. resguardar contra la posibilidad de intrusión y/o de uso no autorizado;
2. asegurar la disponibilidad, confiabilidad, confidencialidad y correcto funcionamiento;
3. ser apto para el desempeño de sus funciones específicas;
4. cumplir las normas de seguridad apropiadas, acordes a estándares internacionales en la materia;

5. cumplir con los estándares técnicos y de auditoria que establezca la Autoridad de Aplicación.

CLAVE CRIPTOGRÁFICA PRIVADA: En un criptosistema asimétrico, es aquella que se utiliza para firmar digitalmente.

CLAVE CRIPTOGRÁFICA PÚBLICA: En un criptosistema asimétrico, es aquella que se utiliza para verificar una firma digital.

INTEGRIDAD: Condición que permite verificar que una información no ha sido alterada por medios desconocidos o no autorizados.

CRIPTOSISTEMA ASIMÉTRICO: Algoritmo que utiliza un "par de claves", una "clave privada" para firmar digitalmente y su correspondiente "clave pública" para verificar dicha "firma digital".

La Ley Modelo de Comercio Electrónico, adoptado por la Comisión de las Naciones Unidas, en el Artículo 2, nos da algunas definiciones.[123]

a) Por "mensaje de datos" se entenderá la información generada, enviada, recibida o archivada o comunicada por medios electrónicos, óptimos o similares,

[123] Texto adoptado por la Comisión de las Naciones Unida para el Derecho Mercantil Internacional en su 29º periodo de sesiones, 28 de mayo a 14 de junio de 1996, Nueva York

como pudieran ser, entre otros, el intercambio electrónico de datos (EDI), el correo electrónico, el telegrama, el telex o el telefax;

b) Por "intercambio electrónico de datos (EDI)" se entenderá la transmisión electrónica de información de una computadora a otra, estando estructurada la información conforme a alguna norma técnica convenida al efecto;

c) Por "iniciador" de un mensaje de datos se entenderá toda persona que, a tenor del mensaje, haya actuado por su cuenta 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 él;

d) Por "destinatario" de un mensaje de datos se entenderá la persona designada por el iniciador para recibir el mensaje, pero que no éste actuando a título de intermediario con respecto a él;

e) Por "intermediario", en relación con un determinado mensaje de datos, se entenderá toda persona que, actuando por cuenta de otra, envíe, reciba o archive dicho mensaje o preste algún otro servicio con respecto a él;

f) Por "sistema de información" se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.

También menciona en el articulo 5 .- Reconocimiento jurídico de los mensajes de datos. No se negarán efectos jurídicos, validez o fuerza obligatoria a la información por la sola razón de que esté en forma de mensaje de datos.

Artículo 9**.** Admisibilidad y fuerza probatoria de los mensajes de datos.

1) En todo trámite legal, no se dará aplicación a regla alguna de la prueba que sea óbice para la admisión como prueba de un mensaje de datos:

a) Por la sola razón de que se trate de un mensaje de datos; o

b) Por razón de no haber sido presentado en su forma original, de ser ese mensaje la mejor prueba que quepa razonablemente esperar de la persona que la presenta.

2) Toda información presentada en forma de mensaje de datos gozará de la debida fuerza probatoria. Al valorar la fuerza probatoria de un mensaje de datos se habrá de tener presente la fiabilidad de la forma en la que se haya generado, archivado o comunicado el mensaje, la fiabilidad de la forma en la 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 10. Conservación de los mensajes de datos.

1) Cuando la ley requiera que ciertos documentos, registro o informaciones sean conservados, ese requisito quedará satisfecho mediante la conservación de los mensajes de datos, siempre que se cumplan las condiciones siguientes:

a) Que la información que contengan sea accesible para su ulterior consulta; y

b) Que el mensaje de datos sea conservado con el formato 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; y

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

2) La obligación de conservar ciertos documentos, registros o informaciones conforme a lo dispuesto en el párrafo 1) no será aplicable a aquellos datos que tengan por única finalidad facilitar el envío o recepción del mensaje.

Artículo 11. Formación y validez de los contratos

1) En la formación de un contrato, de no convenir las partes otra cosa, 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 sola razón de haberse utilizado en su formación un mensaje de datos.

6.3.2. COMUNIDAD EUROPEA.

La producción documental en las organizaciones modernas se produce por medios informáticos y cada vez más se conserva en este tipo de soportes.

Los nuevos soportes conviven en nuestras organizaciones con los documentos en papel, existiendo en gran número de casos duplicidad de soportes por el paso a papel de los documentos electrónicos, y en otros casos a la inversa con la digitalización de documentos.[124]

La principal diferencia con las normas europeas alude a la exigencia de acreditación obligatoria ante el Gobierno de Bolivia. Esto se traduce en la existencia de un solo tipo de firma que siempre será equivalente a lo que se denomina "avanzada" en leyes como la española. Es lógico, porque en Europa la Comunidad es en el hecho un solo país, con una sola moneda y sin barreras aduaneras, donde la confianza y la buena fe son base de sus transacciones comerciales electrónicas. No es igual, por cierto, en los países iberoamericanos, como anticipamos, el proyecto opta por dejar regulado y controlado por el Gobierno de Bolivia el mercado de la certificación electrónica de la identidad de los firmantes, de la misma manera que se súper vigilan a los bancos, a las Universidades, a los agentes de aduana, etcétera.

---

[124] -Todo Derecho - Legislación, jurisprudencia, enlaces, estudios jurídicos, sala de charlas.

Por eso se opta por la necesidad de acreditación obligatoria y la existencia de un solo tipo de firma electrónica, diversa de los mecanismos de autenticación de identidades (claves, biometría) que también se reconocen.

La Comisión Europea ha hecho un pronunciamiento en la Propuesta de Directiva sobre comercio electrónico, en su Artículo 9, señalando la obligación a los Estados de hacer viable la contratación por vía electrónica, y la prohibición hacia los mismos de entorpecer la utilización de los contratos por vía electrónica, o bien de privarlos de efecto y validez en razón de la forma de celebración. En este mismo sentido la Ley Modelo de la Comisión de las Naciones Unidas para el Derecho mercantil Internacional (UNCITRAL o en español CNUDMI) sobre comercio electrónico señala las directrices para otorgar validez al documento electrónico sobre la base de los principios de neutralidad tecnológica y equivalencia funcional.

CONCLUSIONES.

1) El surgimiento de la Informática, y su incorporación a todos los ámbitos de la sociedad, incluyendo también el ámbito jurídico, surgen nuevas relaciones

jurídicas, nuevas figuras jurídicas, y en consecuencia nuevos instrumentos jurídicos y nuevos documentos jurídicos como es el caso de los documentos electrónicos, cuya utilización no esta suficientemente regulada, generando un ambiente nuevo de incertidumbre e inseguridad jurídica.

2) El surgimiento y utilización del Internet, la nueva era trae nuevas relaciones jurídicas con nuevos conflictos y una serie considerable de nuevas controversias difíciles de ser tratados y/o solucionados por falta de una legislación adecuada. En el mundo entero, el Derecho se viene transformando tratando de conseguir ejercer el control social de esas innovaciones, modificando las estructuras legislativas, adecuándose a las nuevas y polémicas cuestiones sociales y jurídicas, y tratando de generar un marco jurídico adecuado de seguridad. Nuestro país aun no ha afrontado decididamente este problema.

3) En las últimas décadas, hay preocupación por reformar las legislaciones avizorando la tipificación de nuevas figuras delictivas de carácter informático. Tal el caso de Bolivia, donde se percibe el interés en proteger al individuo frente la vulnerabilidad existente en los bienes informáticos de los sistemas computarizados. La legislación penal contempla sólo la tipificación de la manipulación informática, la alteración, acceso y uso indebido de datos informáticos. No menciona nada sobre la seguridad que debería existir en un documento electrónico.

4) Esos mecanismos serian instrumentos legales específicos, ya que las actuales disposiciones legales, Decreto Supremo 27328, artículos 363 bis, manipulación informática, articulo 363 ter, alteración, acceso y uso indebido de datos informáticos del Código Penal, articulo 3º de la Ley General de Bancos y Entidades Financieras, no son suficientes para afrontar este problema.

5) La problemática que surge en cuanto a la admisibilidad y valoración de los documentos electrónicos en un proceso judicial, en aquellos casos en que no están expresamente admitidos por la Ley aun no ha sido tratada adecuadamente en términos legales, aun cuando es posible hacer valer en juicio legal los documentos electrónicos. El problema surge, cuando precisamente se trata de documentos que sirven como prueba en un proceso, sin embargo corren el riesgo de ser vulnerados; o no ser admitidos como prueba, incrementando los niveles de inseguridad jurídica de los documentos electrónicos.

6) No existe una adecuada capacitación técnica en aquellas personas vinculadas al Derecho y específicamente en los operadores de administración de justicia, de manera que puedan sentirse seguras al emplear estos medios, y que así puedan brindar seguridad a los ciudadanos.

7) Es probable que ninguna estrategia para la seguridad de los documentos electrónicos tenga éxito: ya que al no existir un mínimo de receptividad política; pero por supuesto no se puede crear receptividad en la sociedad y, el gobierno que es un elemento básico de una estrategia para extender y reforzar la protección en los sistemas informáticos no tiene ayuda especifica sobre este problema.

RECOMENDACIONES.

1) Se debe crear un consejo de alto nivel nacional sobre políticas, estándares, mecanismos de seguridad de autenticación y control, así como seguridad en bases de datos, y sistemas informáticos, donde existen y se ubican a los documentos electrónicos. Este Consejo tendrá básicamente la función de plantear una política o estrategia especifica sobre el problema de la inseguridad de los documentos electrónicos.

2) Nuestro país debe afrontar en forma decidida la posibilidad de una legislación específica que regule el uso y funcionamiento del Internet, que es el instrumento fundamental de transmisión e intercambio de documentos electrónicos y conectar estrategias con el gobierno y personas particulares, así como organismos internacionales para comprometerlos con nuestra propia seguridad.

3) Suscribirse a los nuevos tratados internacionales y en su caso, elevarlos a rango de Ley dedicadas a la protección de los documentos electrónicos, podría incrementar la confianza y la seguridad de las personas en cuanto a estos documentos.

4) La certificación de firma electrónica, a través de una autoridad certificante por su importancia en el avance de la tecnología, debe ser obligatoria y de carácter general para todos, siendo así, permitiría identificar inequívocamente al firmante del documento electrónico, evitando la posibilidad del posterior repudio o alternativamente de fraude o daños patrimoniales

.

5) Los notarios de fe pública deben concentrarse en su actividad de asesorar, interpretar la voluntad, de dar forma, de legalizar, legitimar y sobre todo de dar fe publica en la creación de documentos electrónicos auténticos. El papel de los notarios electrónicos es clave para la seguridad jurídica de los documentos electrónicos, por lo que debe ya instalarse, mediante Ley expresa, los notarios electrónicos.-

BIBLIOGRAFÍA.

AZPILCUETA, Hermilio. Derecho Informático, Ed. Abeledo- Perrot Buenos aires Argentina, 1987. 18-30.

BISHOP, M. (2003) Computer Security. Art and Science. Addison Wesley

CANO, J. (2000) Programación Segura? Conceptos y Aspectos Técnicos. Conferencia Magistral. Congreso Nacional de Estudiantes de Ingeniería de Sistemas. Santa fe de Bogotá. Colombia. Universidad Distrital.

CANO, J. (2004) Hacia un concepto extendido de la mente segura. Pensamiento sistémico en seguridad informática. Artículo de investigación (En revisión). Universidad de los Andes

CARNELUTTI, Francesco, Las miserias del proceso penal (Trad. de Santiago Sentis Melendo). Bogotá, Temis, 1989, XIV-107 p.p. (Monografías jurídicas, segunda serie, número 55).

CORREA, Carlos. Derecho Informático Ed. Depalma Buenos Aires Argentina, 1993. 30-42. 85-96.

DAVARA Rodríguez, Miguel Ángel. Derecho Informático. España. Editorial Aranzadi, 1993.

GHERSI, Carlos. Derecho de Daños, Ed. Abeledo - Perrot Buenos Aires Argentina, 1999.

GOLLMAN, D. (1999) Computer security. John Wiley and Sons.

GONZALES Hernández, Horacio Jesús. Valor Probatorio del Documento Electrónico. Maracaibo: Universidad del Zulia, Facultad de Ciencias Jurídicas y Políticas, Dirección de Seminarios, 2000. pp.259 (Tesis Doctoral)

GRÜN, Ernesto, Una visión sistémica y cibernética del Derecho. Buenos Aires, Abeledo-Perrot, 1995, 122 p.p.

HANCE, Olivier, Leyes y negocios en Internet. (Trad. De Yazmin Juarez Parra). México, McGraw Hill, 1996, 371 p.p.

JURISPRUDENCIA Argentina.-Tomo II- Año 1999- "Documento Electrónico" por Daniel Altmark, págs. 851-855.

HAWKRIDGE, David. Informática y Educación. Las nuevas tecnologías de la información. Ed. Abeledo- Perrot. Buenos. Aires Argentina ,1992.

LEDESMA, Guillermo. Derecho Penal. Parte Especial. Ed. Abeledo - Perrot. Buenos Aires - Argentina, 1995.

MEJAN, Luis Manuel C., El Derecho a la intimidad y la informática. 2º ed., México, Porrúa, 1996, XXII-146 p.p.

MOLINA Salgado, Jesús Antonio, Delitos y otros ilícitos informáticos en el Derecho de la Propiedad Industrial. México, Porrúa, 2003, XVI-107 p.p. (Breviarios Jurídicos, número 7).

MANTOVANI, Fernando. El siglo XX y las ciencias criminales. Ed. Temis S.A. Bogota Colombia, 1998.

OECD: Organización para la Cooperación Económica y el Desarrollo. In: Computer related criminalliy: analisys of legal policy in the OECD area, ICCP, 84:22, 1984.

OZORES, Isabel. La superautopista de la Información. Más allá del Internet., Ed. Peter Otte, Madrid España 1995.

PACHECO Escobedo, Alberto, “La contratación por medios electrónicos”, en Homenaje a Manuel Borja Martínez. México, Porrúa, Colegio de Notarios del Distrito Federal, 1992, pag. 207 a 231.

PEREZ, Luño, Antonio Enrique. Manual de informática y Derecho. Editorial Ariel S.A, Barcelona, 1991. P.82-103.

PEREZ Luño, Antonio Enrique, Ensayos de Informática Jurídica. México, Fontamara, 1996, 151 p.p.(Biblioteca de Ética, Filosofía del Derecho y Política, número 46).

RIVERA Llano, Abelardo, Dimensiones de la informática en el Derecho. (Perspectivas y problemas). Santa fe de Bogotá, Jurídica Radar, 1995, XVIII-285 p.p.

ROSZAK, Theodore, El culto a la información. El folclore de los ordenadores y el verdadero arte de pensar. (Trad. de Jordi Beltrán). México, Consejo Nacional para la Cultura y las Artes, Grijalbo, 1990, 277 p.p.

TÉLLEZ Valdez, Julio, Derecho Informático. 2º ed., México, McGraw Hill, 1995, XII-283 p.p. (Serie Jurídica).

TELLEZ Valdez, Julio. Derecho Informático, Ed. Mc. Graw - Hill México. 1997 p.56-70.

ZAFFARONI, Eugenio Raúl, Manual de Derecho Penal. Parte General. Ed. Ediar, Buenos Aires Argentina. 1987.

ZANELLATO Marco Antonio. In: Conductas ilícitas na sociedade digital. Caderno Jurídico Direito e Intenet - Ed. Imprensa Oficial do Estado - julho 2002. Escola Superior do Ministério Público de São Paulo. P. 189.

ENCICLOPEDIAS Y DICCIONARIOS

ENCARTA.- Enciclopedia electrónica. 2003

OMEBA.- Enciclopedia Electrónica Jurídica.- Argentina 2002.

LAROUSSE.- Diccionario Ilustrado.- Argentina.

MENTOR INTERACTIVO.- Océano.- Enciclopedia temática estudiantil. España.2004.

WIKIPEDIA, la enciclopedia libre.

LEYES Y CONVENIOS

CONSTITUCIÓN POLÍTICA DEL ESTADO

CÓDIGO PENAL BOLIVIANO

CÓDIGO CIVIL BOLIVIANO

CÓDIGO DE PROCEDIMIENTO CIVIL

DECRETO SUPREMO 27328

PROYECTO DE LEY DE DOCUMENTOS, FIRMAS Y COMERCIO ELECTRÓNICO. PRESIDENTE EVO MORALES AIMA.

LEY 19799-CHILE

TEXTO ORDENADO DE LA LEY No 1488 DE BANCOS Y ENTIDADES FINANCIERAS

REAL DECRETO- LEY 14/1999-ESPAÑA

LEY MODELO DE FIRMA DIGITAL. O.N.U.

LEY MODELO DE COMERCIO ELECTRÓNICO

PAGINAS WEB

-I A C I S (International Association of Computer Investigative Specialist)- http://www.cops.org- y la H T C N – http://www.icsa.com

-Really. http://www.securecoding.org/

-Estrategias de Seguridad. Benson Christopher (Inobis Consulting Pty Ltd). Microsoft© Solutions. Noviembre 2000. http://www.microsoft.com/latam/technet/articulos/200011

-Gonzales, Miguel F. Dantowitz, Roberto. Rugna, Daniel. Monografía "Seguridad en Internet". Facultad de Ingeniería. UBA. Primer cuatrimestre 1998. Buenos Aires. Argentina. http://cactus.fi.uba.ar/crypto/tp_ant.html

-Schneier, Bruce. Criptograma. Edición mensual kriptopolis.org. Marzo 1999-Julio 2001. http://www.kriptopolis.org/criptogram

-Anonimo. Maximum Security. A Hacker's guide to protecting your Internet Site and Network. Macmillan Computer Publishing©. 1999. EE.UU. http://sams.net –

-http://www.ods.com.ua/win/eng/security/Max_Security -
http://www.itlibrary.com/reference/library/1575212684/ewtoc.html

-ArCERT. Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública. Manual de seguridad en redes. Argentina. 2000. http://www.arcert.gov.ar

-DerechoGratis - Consultas e información sobre legislación y jurisprudencia.

-El Boga - Leyes, agrupaciones, organizaciones, constituciones internacionales y otros recursos.
-Todo Derecho - Legislación, jurisprudencia, enlaces, estudios jurídicos, sala de charlas.

-www.monografias.com/trabajos/histocomp/histocomp.shtml

-www.alfa-redi.org/documento/default.asp

Historia de la Era de la Computación Home | Prólogo | Prehistoria | Siglos XIV al XIX | 1a Generación| 2a Gen. | 3a Gen. | 4a Gen.| Las PC | Internet |. Jorge Machado ...
www.perantivirus.com/historia/