

K845
E44P47

UNIVERSIDAD DE LOS ANDES
FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS
ESPECIALIZACIÓN DE DERECHO MERCANTIL



LA CONTRATACIÓN ELECTRÓNICA
Y SUS DELITOS EN LAS SOCIEDADES ANÓNIMAS DE VENEZUELA

Trabajo Especial de Grado, como requisito parcial para optar el
Grado de Especialista en Derecho Mercantil

Mención Sociedades

www.bdigital.ula.ve

Autor: Abg. María Emilia Perdomo Villegas

Tutor: Prof. Dr. José Luis Malaguera Rojas

Mérida, Noviembre de 2.012

Atribución - No Comercial - Compartir Igual 3.0 Venezuela
(CC BY - NC - SA 3.0 VE)



UNIVERSIDAD DE LOS ANDES
FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS
ESPECIALIZACIÓN DE DERECHO MERCANTIL
MÉRIDA ESTADO MÉRIDA

APROBACIÓN DEL TUTOR ACADEMICO

En mi carácter de tutor del trabajo especial de grado titulado: **LA CONTRATACIÓN ELECTRÓNICA Y SUS DELITOS EN LAS SOCIEDADES ANÓNIMAS DE VENEZUELA**, presentado por la Abogada: María Emilia Perdomo Villegas, portadora de la cédula de identidad N° V-16.276.968, quien opta al grado de Especialista en Derecho Mercantil Mención Sociedades que otorga la ilustre Universidad de los Andes y considerando que dicho Trabajo de Grado reúne los requisitos y méritos suficientes; apruebo que el mismo sea sometido a la presentación pública y evaluación por parte del jurado examinador que le sea designado.

En Mérida, a los treinta (30) días del mes de noviembre de 2012.

Prof. Dr. José Luis Malaguera Rojas
C.I. V-5.206.852

DEDICATORIA

A mis padres, hermanos y toda mi familia, en especial a mi esposo
e hija, quienes son mi fuente de estímulo y superación.

www.bdigital.ula.ve

AGRADECIMIENTO

Mis sinceras palabras de agradecimiento

A Dios Todopoderoso, por darme la vida y protegerme en todo momento

A La Universidad de Los Andes, valiosa casa de estudios que me ha formado

Al Dr. Prof. Ricardo Moreno, Excelente Coordinador de Post-Grado

Al Dr. Prof. José Luis Malaguera Rojas, a quien admiro y respeto, por su valioso aporte que mejoró esta investigación

A la Dra. Prof. Gauris Vela, por sus enriquecedores conocimientos

A mis compañeros de Postgrado, respetables colegas

A mi madrina Zarait, por su apoyo incondicional en esta meta, eres un excelente ejemplo para mí, te quiero mucho

A mi hermosa familia, que siempre confió en mí, los amo mucho

A todos Ustedes ¡Gracias, por formar parte de mi vida!

INDICE DE CONTENIDO

	pp.
Carta de aprobación del tutor académico.....	ii
Carta de aprobación del tutor metodológico.....	iii
Dedicatoria.....	iv
Agradecimiento.....	v
Resumen.....	viii
Introducción.....	1

CAPITULO

I. EL PROBLEMA

Planteamiento del Problema.....	4
Objetivos de la Investigación.....	8
Objetivo General	
Objetivos Específicos	
Justificación de la Investigación.....	9
Alcances.....	10

II. ESTADO ACTUAL DE LA INVESTIGACIÓN

Antecedentes.....	12
Bases teóricas.....	17
Bases Legales.....	37
Unidad de Análisis.....	44

III. MARCO METODOLÓGICO

Tipo y Diseño de la Investigación.....	45
Recolección y Selección de la Investigación.....	46
Procedimientos de la Investigación.....	47

IV. DESARROLLO Y DISCUSIÓN

Interpretación de la información recabada. Análisis crítico y reflexivo... 50	
---	--

V. CONCLUSIONES Y RECOMENDACIONES

Conclusiones.....	90
Recomendaciones.....	92
REFERENCIAS.....	94

www.bdigital.ula.ve

UNIVERSIDAD DE LOS ANDES
FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS
Especialización en Derecho Mercantil
Mención Sociedades

LA CONTRATACIÓN ELECTRÓNICA
Y SUS DELITOS EN LA SOCIEDADES ANÓNIMAS DE VENEZUELA

Autor: Abg. Maria Emilia Perdomo Villegas

Tutor: Prof. Dr. José Luis Malaguera Rojas

Fecha: Noviembre 2012.

RESUMEN

En la actualidad un sinnúmero de empresas realizan diariamente operaciones electrónicas relacionadas con la compra-venta de bienes y servicios, transacciones bancarias, transmisión de datos, publicidad, entre otros, de allí la importancia para la vida económica, financiera, social y cultural de un país el buen uso de las Tecnologías de Información y Comunicaciones, ante este contexto la presente investigación tiene como propósito analizar la contratación electrónica y sus delitos en las sociedades anónimas venezolanas. El estudio se realizó con una investigación documental bajo un diseño de tipo descriptivo, prestando especial atención al ordenamiento jurídico positivo vigente que regula esta materia y los sistemas de seguridad más comunes diseñados hasta el momento, como mecanismo de prevención para evitar la comisión de delitos relacionados con esta actividad. Los resultados obtenidos permitieron conocer que a través de la Ley sobre Mensajes de datos y Firmas Electrónicas se consagra el reconocimiento jurídico y eficacia probatoria del documento electrónico y la firma electrónica, además los sistemas de seguridad son fundamentales para que las empresas y consumidores tengan confianza en la privacidad de sus transacciones siempre que sean accesibles, legales y seguros, permitiendo el mayor desarrollo del comercio electrónico, se describe la estructura típica de los delitos en esta actividad, reafirmando que de todas las defraudaciones informáticas, el delito de estafa es el más frecuente, del mismo modo se caracterizan algunas modalidades y medios de comisión, indicándose algunas recomendaciones para su precaución.

Descriptores: Contratación Electrónica, Delitos, Sociedad Anónima.

INTRODUCCIÓN

El desarrollo tecnológico que se viene logrando en los países industrializados, permite agilizar y hacer más operante la prestación de servicios y el intercambio de bienes tangibles e intangibles lo cual hace importante que nuestro país incorpore normas que faciliten las condiciones para acceder a canales eficientes de derecho mercantil internacional, el proceso de contratación electrónica resulto ser uno de los más importantes en el desarrollo de la sociedad de la información, es por ello que en Venezuela, la Ley sobre Mensajes de Datos y Firmas Electrónicas reconoce la eficacia y le da validez jurídica tanto al mensaje de datos como a la firma electrónica otorgándole al documento electrónico el mismo valor probatorio que al documento manuscrito.

Como bien lo señala, Salgueiro (2001) "La Ley sobre Mensajes de Datos y Firmas Electrónicas ha pasado a constituir una herramienta indispensable para que nuestro país se mantenga a la vanguardia regional en materia de derecho adaptado y aplicado a las nuevas tecnologías."

El uso regular de la informática para la comunicación entre las personas, como medio válido para manifestar su voluntad así como para contraer derechos y obligaciones ha traído como consecuencia la necesidad de que el derecho se adapte a estas nuevas realidades dándole un reconocimiento y un valor a los actos provenientes de la Red.

La investigación que se presenta, pretende analizar la contratación electrónica y sus delitos en las sociedades anónimas venezolanas y para ello se abordan temas esenciales como la naturaleza jurídica del contrato electrónico, formación del contrato electrónico, haciendo énfasis en los elementos de la oferta y aceptación, la valoración jurídica del documento

electrónico, igualmente desde un punto de vista más técnico se analizarán los sistemas criptográficos (simétrico y asimétrico), la firma electrónica, la biometría, como sistemas de seguridad más comunes para evitar ser víctima de fraudes electrónicos, ultimando con abordar los delitos cometidos en contratación electrónica, como son: la oferta engañosa, la estafa y el fraude electrónico.

La presente investigación se encuentra estructurada en cinco capítulos:

Comenzando con el Primer Capítulo, referido al planteamiento del problema, que permitirá visualizar el estudio partiendo de un ámbito internacional hasta llegar al ámbito nacional como es Venezuela, incluye igualmente los objetivos de la investigación, la justificación y los alcances; El Objetivo Principal, es analizar la contratación electrónica y sus delitos, para que con ello las sociedades anónimas tengan un criterio formado como parte contratante "on line", ya que ante la aparente simplicidad del mecanismo de los contratos electrónicos, especialmente el contrato de compraventa, se ha constatado que producen problemas tanto de carácter práctico como legal que requieren de conocimientos mínimos que permitan a este tipo de empresas como desenvolverse y exigir sus derechos.

El segundo capítulo, alude al marco referencial, en donde se ubicaran los antecedentes de esta investigación, así como, las teorías que apoyan la línea de investigación, como son: principalmente las sociedades anónimas, los contratos y los delitos relacionados con la contratación electrónica, igualmente, las bases legales o legislación aplicable en esta materia.

El tercer capítulo, da a conocer la metodología que permitió desarrollar esta investigación, como fue la de investigación documental bajo un diseño

de tipo descriptivo, igualmente se describe el método, técnicas y procedimientos utilizados en esta investigación.

El cuarto capítulo plantea el desarrollo y discusión de la investigación. Para ello se desarrollarán los objetivos específicos: Se realizó un análisis de la contratación electrónica de acuerdo a la regulación jurídica en Venezuela, sus elementos, haciendo especial énfasis al consentimiento, la oferta y aceptación, el valor probatorio de los mensajes de datos, igualmente, se analizará la firma electrónica como mecanismo para certificar la identidad de los contratantes, así como, se analizarán los sistemas de seguridad en Internet para evitar delitos, luego abordaremos en particular el estudio de los tipos penales aplicables a la contratación electrónica y sus consecuencias,.

El quinto capítulo finalizó con las conclusiones y recomendaciones para luego presentar las referencias utilizadas.

www.bdigital.ula.ve

CAPITULO I

PLANTEAMIENTO DEL PROBLEMA

A mediados de los noventa cuando empezó a nivel mundial la utilización de Internet con fines comerciales, nadie habría sido capaz de predecir el efecto que tendría sobre el mundo de los negocios. Los sitios Web se consideraban como un complemento, los correos electrónicos se percibían con desconfianza y muchos lo miraban como algo impreciso y poco práctico para la comunicación. Hoy día las cosas han cambiado, millones de personas en el mundo usan Internet habitualmente y se espera que cualquier empresa digna de tal nombre tenga un dominio en la Red.

Una de las consecuencias del uso de los avances tecnológicos de información y telecomunicaciones es, que se han producido nuevos tipos de contrataciones o transacciones, que muchas son análogas a las efectuadas a través de medios tradicionales, puesto que, son sólo mecanismos modernos de comunicación que pueden ser utilizados para cualquier tipo de transacción.

Este nuevo mecanismo moderno de comunicación, capaz de convertirse en contratos electrónicos y tener los mismos efectos jurídicos que un contrato tradicional, se reflejó en la evolución legislativa mundial de los últimos años que fue desarrollada por los países, entre ellos Venezuela, cuya manifestación de derecho regulatorio a nivel mundial, partió inicialmente con los organismos internacionales, así; la Organización de las Naciones Unidas (ONU), en los años ochenta promulgó la Ley Modelo para el Comercio Electrónico de UNICITRAL, creada con la intención de que los países unificaran criterios al adoptar normas de derecho interno vinculadas con este asunto, este mismo organismo dictó, a principios de los noventa, normas de

seguridad para los sistemas informáticos con la Organización de Cooperación para el Desarrollo Económico (OCDE), entre otros, y a nivel nacional con la promulgación de la Ley sobre Mensajes de Datos y Firmas Electrónicas del año 2001, quien adoptó muchas de las recomendaciones de la ONU. Todas estas iniciativas estuvieron enmarcadas bajo la tendencia prevaleciente de estimular y fortalecer la interconexión, el desarrollo armónico de las tecnologías de información como instrumento de desarrollo, incentivar las transacciones el intercambio de bienes y servicios, en fin, la procura del desarrollo del comercio electrónico.

Sin embargo, comenzaron a sentirse los efectos de conductas dañosas que afectaban bienes jurídicos relevantes, resultando inocultable la percepción de que la red no podía ser tan segura como parecía, representando un peligro, al respecto Ditotto (2010) señala:

Este nuevo concepto de documento se reflejó en la evolución legislativa mundial de los últimos años que fue desarrollada por los países justamente para aprovechar las ventajas de las tecnologías de información. Por este mismo motivo, las primeras manifestaciones fueron de derecho regulatorio, signadas por el ánimo de incentivar las transacciones, los intercambios de bienes y servicios, en fin, la procura del desarrollo del comercio electrónico. Al margen de todo esto comenzaron a manifestarse conductas inconvenientes, abusivas, derivadas de tanta libertad, de la propia dinámica muy democrática, pero un tanto caótica que ha caracterizado la expansión de las tecnologías de información.

Como se aprecia, este fenómeno tecnológico, además de traer múltiples beneficios, plantea problemas jurídicos inéditos que en principio encuentran solución por vía analógica en el Código Civil, Código de Comercio y Código Penal, sin embargo, la velocidad y el continuo desarrollo de nuevas tecnologías hacen que la regulación vigente parezca insuficiente o anticuada, por lo siguiente: el uso masivo de las tecnologías para adquirir bienes y/o servicios y la utilización de las Tecnologías de Información y

Telecomunicaciones para cometer ilegalidades o delitos, siendo en este punto donde se le abre paso al derecho penal sancionatorio.

Las ampliaciones a los conceptos tradicionales, para que la protección legal se adecue a las necesidades de los avances tecnológicos, se sustenta en el interés de brindar seguridad y confianza principalmente a los negocios jurídicos que se desarrollen a través de estas nuevas tecnologías, ya que, los mismos, conllevan a la comisión de ciertos hechos o actos considerados por nuestra legislación positiva vigente como delitos informáticos, en los cuales la intervención de las sociedades anónimas no son ajenas a ellos, bien sea como sujeto activo o pasivo de delito, afectando intereses relacionados directamente con bienes jurídicos protegidos, como son: el derecho de propiedad, derecho al acceso de la información, el orden económico, derecho a la intimidad, derecho a la honra y al buen nombre, etc.

Esta situación planteada incide directamente con ciertas conductas desplegadas, como son: la posibilidad de eliminar, agregar o modificar, transacciones en forma dolosa o fraudulenta, pudiendo violarse secretos importantes de una empresa, los motivos son explicados claramente por Gabaldon y Becerra (2008), al señalar:

Esto ocurre debido a que mucha de la información sensible viaja a través de la red, lo que permite la usurpación de la identidad, el revelar involuntariamente información confidencial, la difusión y venta de información confidencial no autorizada, los portales falsos o empresas inexistentes y el espionaje, entre otros.

Esta situación representa una amenaza a los derechos de seguridad y privacidad de las personas, por ejemplo: en las compras hechas por Internet se suministran datos personales, tales como: nombre, dirección, teléfono y número de tarjeta de crédito, situación que expone al comprador a que se

vincule su identidad con los bienes o servicios adquiridos, pudiendo el vendedor o proveedor, vender dicha información a otras compañías dedicadas a la publicidad directa o negocios alternos, entre otros.

Existen muchos riesgos para las compañías anónimas que ofrecen servicios electrónicos, estos pueden presentarse por deficiencias en el sistema de seguridad, falta de políticas de gestión de riesgo, falta o insuficiencia de tecnología, falla en los servicios del proveedor o falta de precaución por parte del cliente, asociándose a la introducción de virus, robo de datos, fraudes, estafas y otros ataques, también se genera, la publicidad negativa sobre la empresa o cualquiera de sus productos o servicios, o para el sector en general, cuando se presentan frecuentes carencias o fallan los sistemas de seguridad. Creando este escenario en ocasiones, violación o incumplimiento de alguna disposición legal, o cuando los derechos y obligaciones de las partes en las operaciones electrónicas no se encuentran bien definidos, lo cual genera incertidumbre y falta de confianza para hacer uso de este tipo de operaciones.

Ante esta problemática social y jurídica es que surge la necesidad de identificar esas conductas delictivas que se forman con la actividad de contratar electrónicamente en las sociedades anónimas, para subsumirla a los tipos penales actuales, los cuales se encuentran disgregados en nuestra legislación vigente y así crear una adecuada cultura de conocimiento y prevención de delito.

En este mismo orden de ideas, cabe interrogarse ¿será factible compilar todas estas conductas fraudulentas en un solo cuerpo legal?, sería muy interesante tanto para el profesional del derecho como para todo aquel interesado en realizar contrataciones a través del uso de las tecnologías de

la información y las comunicaciones, puesto que, con un cuerpo normativo de tal magnitud, fortalece el conocimiento general en esta materia.

De acuerdo a lo anteriormente expuesto, la presente investigación queda formulada bajo las siguientes interrogantes: ¿Cómo es la contratación electrónica y sus delitos en las sociedades anónimas Venezolanas?, ¿Existe regulación jurídica en Venezuela de los contratos electrónicos?, ¿Cuáles son los sistemas de seguridad en Internet para evitar delitos en los contratos electrónicos?, ¿Qué delitos se pueden cometer con el contrato electrónico?, interrogantes que conducen a realizar esta investigación con el fin de establecer con bases teóricas y jurídicas los pro y los contra de esta nueva forma de contratar además de, generar razonamientos que contribuyan a mejorar la problemática planteada. Desarrollando los objetivos específicos, se les dará respuesta a estas interrogantes.

Objetivos de la Investigación

Objetivo General:

Analizar la contratación electrónica y sus delitos en las sociedades anónimas de Venezuela

Objetivos Específicos

- (a) Analizar exhaustivamente la regulación jurídica de la contratación electrónica para las sociedades anónimas en Venezuela.
- (b) Estudiar analíticamente los sistemas de seguridad en Internet para evitar los delitos en los contratos electrónicos.

- (c) Desarrollar de manera crítica los tipos penales aplicables a la contratación electrónica.

Justificación de la Investigación

Desde el punto de vista social, esta investigación es relevante en virtud, de que está vinculada con el actual contexto de la Sociedad de la Información, la información se ha convertido en el cuarto factor económico superando a las materias primas: tierra, trabajo y capital, asimismo, el contrato es el instrumento por excelencia para que el hombre en sociedad pueda satisfacer sus necesidades, ante estas dos particularidades se infiere la necesidad del desarrollo de esta cultura técnica, dado que importa un nuevo paradigma en la negociación y en los sistemas de contrataciones implica un cambio cultural.

Además, es importante señalar que en un mercado electrónico cada vez más global, productores, intermediarios y consumidores, deben conocer sus derechos y obligaciones, así como el tipo de reparación que pueda obtener en caso de violación de sus derechos o de incumplimiento de obligaciones.

Sin el uso de los contratos no se podría concebir la realización de la vida económica en las comunidades organizadas, y desde el punto de vista económico, el uso de los avances tecnológicos facilita el progreso en las empresas y la agilización de las relaciones comerciales con los adquirentes de los bienes, al mejorar el servicio, la calidad de los productos y la atención al cliente, como se aprecia es un tema muy novedoso, en razón de lo anterior, se considera de vital importancia para la vida de las empresas, tener el conocimiento necesario para realizar contrataciones electrónicas exitosas, evitando las conductas delictuosas, para el control de sus ganancias.

Con esta investigación, una vez más se motiva a que los legisladores llenen ese vacío regulatorio en materia de contratación adaptado a las nuevas tecnologías y se armonice con las normas existentes, para facilitar las condiciones en el acceso a canales eficientes de derecho mercantil internacional, así como, brindar los márgenes indispensables de seguridad en los negocios y comunicaciones.

Alcances de la Investigación

Los alcances de la presente investigación, circunda en analizar la contratación electrónica, percibida como una nueva actividad para que las empresas y en especial las sociedades anónimas puedan responder eficazmente a las exigencias planteadas por la creciente globalización, por tal motivo este estudio busca conocer si la Ley sobre mensajes de datos y firmas electrónicas, engloba las exigencias legales que en la práctica se necesitan para darle validez a este tipo de contrato.

Igualmente, con el análisis de los sistemas de seguridad en Internet para evitar delitos y los tipos penales que en Venezuela se aplican para esta nueva forma de contratar, empleando doctrina, leyes, jurisprudencia y descripción de modalidades de comisión de delito, se permite constatar si existen lagunas jurídicas desde el punto de vista del derecho penal sancionatorio, por tal motivo, en términos geográficos, la presente investigación tendrá un alcance nacional, específicamente en el sistema legislativo venezolano.

En atención a lo antes expuesto, los métodos empleados tienen repercusión directa en la eficacia de los aportes teóricos, estando este estudio enmarcado con base en las ciencias jurídicas, principalmente en el

área de Derecho Mercantil relacionándose con el Derecho Civil y Penal, vinculado al contrato electrónico y sus delitos, para que con ello las empresas se planteen retos de actualización, procurando siempre el debido respeto a los regímenes jurídicos tanto nacionales como internacionales y así estén acordes con los cambios de orden social, económico, regional y mundial. Esto con la finalidad de facilitar tanto al jurista venezolano como a cualquier interesado, una herramienta de trabajo que amplíe y profundice el conocimiento global de este nuevo fenómeno tecnológico en el mundo de los contratos.

www.bdigital.ula.ve

CAPITULO II

ESTADO ACTUAL DE LA INVESTIGACION

ANTECEDENTES

Es innegable que la presencia de la Internet en el mundo global que sobrelleva a las transacciones electrónicas, representa para las empresas una vía innovadora para su crecimiento y desarrollo, no obstante, toda investigación cuenta con un conjunto de antecedentes que constituyen los estudios previos que permiten tener una visión apropiada a encaminar el problema planteado, para así tener criterios que conlleven a determinar la trascendencia del estudio en cuestión. A continuación se exponen los principales antecedentes encontrados:

En primer lugar, se cita a la venezolana Rico (2005) en su obra documental titulada "Comercio Electrónico, Internet y Derecho" mediante el cual aborda aspectos centrales del comercio electrónico en su dimensión contractual y suministra conocimientos básicos sobre su funcionamiento técnico, enfocándose en su estudio predominante de Derecho privado, apunta la importancia de las nuevas tecnologías, analiza el marco conceptual del comercio electrónico en general y explica desde el punto de vista técnico teórico el funcionamiento de Internet y su influencia en el desarrollo del comercio electrónico, con mención a los principales problemas que presenta emprende el estudio de la documentación electrónica de los actos jurídicos y la importancia de su tratamiento como medio de prueba, concluye con el estudio de la seguridad desde el punto de vista técnico-jurídico.

Esta obra es de interés para la presente investigación, ya que del estudio del perfeccionamiento del contrato electrónico, se observa la

distinción que hace esta autora de las fases para la formación y ejecución de estos contratos, igualmente se obtendrá los principales sistemas de seguridad usados en Internet, desde un punto de vista más técnico, como mecanismo de prevención de delitos.

Continuando con Rincón (2006), con su obra literaria “Contratación Electrónica”, estudia diversos aspectos relacionados con la contratación electrónica, procesos licitatorios electrónicos, contratación pública por medios electrónicos en Colombia, implicación del comercio electrónico dentro de la tendencia de las telecomunicaciones, la formación del consentimiento en materia de contratación electrónica, señalando que los elementos de la oferta y la aceptación, podrán ser expresados por medio de mensajes de datos, igualmente explica los sistemas de aceptación para este tipo de contratos a distancia o entre ausentes, realiza una investigación de tipo documental.

Esta obra literaria, es relevante para este estudio, en virtud de que se toma de ella los requisitos necesarios para que se forme el consentimiento y circunstancias que se vinculan con la aceptación electrónica propiamente dicha.

Lozada (2010), estudia la importancia y validez del contrato electrónico en el ordenamiento jurídico venezolano y su relación con el comercio electrónico. Trabajo Especial del Grado de la Universidad de los Andes, Mérida – Venezuela. En su obra, analiza e identifica los principales contratos electrónicos e informáticos y su relación con el Internet específicamente en cuanto a sus suficiencias e insuficiencias normativas y regulativas y estudia de manera crítica la validez de los contratos electrónicos en la legislación venezolana, afirmando que la celebración del contrato a través de medios electrónicos, encuentra su fuente y reconocimiento jurídico en el texto de la

Ley sobre mensajes de datos y firmas electrónicas en su artículo 15, realiza una investigación documental, bajo un diseño bibliográfico tipo descriptivo.

Este estudio se considera importante para la presente investigación, por cuanto del mismo se conseguirá delimitar los requisitos puntuales, tanto para la oferta como para la aceptación, en lo que respecta a la formación del contrato, como elemento para la validez del contrato electrónico, referido a la manifestación del consentimiento.

Con relación a los delitos que provienen del comercio electrónico, encontramos el Trabajo Especial de Grado de Díaz (2008), titulado "Lineamiento para una propuesta de normativa jurídica que regule a las sociedades mercantiles como sujetos activos de delito en el comercio electrónico a partir del análisis comparativo con el Derecho Español" donde realiza un estudio comparativo, ante la necesidad de introducir reformas en la legislación venezolana para la regulación del comercio electrónico, toma como parámetros de comparación por Venezuela la Ley sobre Mensaje de Datos y Firmas Electrónicas y la Ley Especial contra los Delitos Informáticos y por España la Ley 59/2003 del 19 de diciembre, logra establecer unos lineamientos para una propuesta de normativa jurídica aplicada a las sociedades mercantiles en Venezuela relacionados con el objeto y aplicación de la Ley, definiciones, efectos jurídicos de la firma electrónica, requisitos del certificado electrónico, sanciones y tipos penales, la metodología empleada en esta investigación se encuentra enmarcada en la modalidad de Proyecto Factible con carácter descriptivo bajo un diseño de investigación prospectivo.

Este estudio, contribuye al esclarecimiento del desarrollo de las conductas delictivas en el manejo de las contrataciones electrónicas en las que pudiera ser víctima o sujeto activo de delito, las compañías anónimas en cuestión y se comparte la afirmación de que en Venezuela la Ley Especial

contra los Delitos Informáticos, como norma jurídica penal que regula el comercio electrónico, presenta un vacío jurídico en relación a la firma electrónica, pues no presenta su definición ni esta regulada en ninguna de sus formas, pudiendo patentarse el delito de falsificación de firma electrónica que es el más común en el tipo de fraude.

Por su parte, Zapata (2009), con su Trabajo Especial de Grado, titulado “El delito de Estafa en la modalidad de Phishing a través de internet y sus medios probatorios en Venezuela”, de la Universidad de Carabobo, indagó sobre esta modalidad de estafa informática que consiste en duplicar una pagina web de la banca, institución financiera o de una tienda en Internet para ser utilizada en forma fraudulenta, a través del envío de correos electrónicos, destaca los medios de prueba derivados de las nuevas tecnologías de información, las repercusiones sociales y económicas de este delito para enfrentarlo y examina el derecho comparado en esta materia, la modalidad que utilizó para esta investigación es descriptiva – informativa, con un diseño de tipo documental, puesto que explica con casos prácticos esta forma de delinquir basándose igualmente en textos, trabajos de grados y ponencias.

Esta investigación es importante para el estudio del presente trabajo, pues el delito de estafa es uno de los tipos penales que se caracterizarán en el desarrollo de esta investigación como uno de los delitos aplicables a la contratación electrónica, por tal motivo, se considera útil definir y explicar la modalidad de phishing y su principal forma de ejercerla, aunado a ello, este autor sostiene la dificultad que enfrenta hoy día el sistema penal venezolano para darle admisibilidad y apreciación a los elementos de convicción, pues no radica en restricciones establecidas por el ordenamiento jurídico, sino que esta dificultad se relaciona con la poca cultura tecnológica que muchas veces los sujetos procesales, aún cuando tiene la potestad de conducir una

investigación, carecen de conocimientos especializados para comprenderlos e interpretarlos, por ello, se considera notorio el necesario auxilio de los expertos para la traducción específica del significado de un rastro contenido en soportes lógicos y no físicos.

En este mismo orden, Granadillo (2008) en su obra “Delitos Bancarios”, comentó los tipos penales establecidos en la Ley General de Bancos y otras Instituciones Financieras, hoy denominada Ley de Instituciones del Sector Bancario, con esta indagación dicha autora afirma, que el orden económico es uno de los pilares fundamentales que sustenta el funcionamiento y la estabilidad de los Estados, siendo por ello de vital importancia la legislación tendente a proteger la actividad fiscal, monetaria y bancaria, esta obra se orienta fundamentalmente a convertirse en un aporte dentro de la denominada legislación penal colateral con su respectiva incidencia en lo relativo a la materia de derecho penal bancario. Realiza una investigación de tipo documental, por cuanto desarrolla lo atinente a la especialidad de la materia penal bancaria, con exclusivo énfasis al análisis sobre los tipos penales previstos en la legislación venezolana.

Cabe significar, que esta obra literaria tiene un gran aporte a la presente investigación, por cuanto, se comparte la afirmación de esta autora de atribuirle carácter doloso al delito de fraude electrónico, (tipo penal que será objeto de estudio en este trabajo) y considerarlo un delito que atenta más contra la entidad bancaria que contra clientes o usuarios, pues cuando la acción va desplegada a estos últimos, pudiera ser subsumible en el delito de Fraude que tipifica el artículo 14 de la Ley Contra los Delitos Informáticos, además se toma en consideración el estudio de la estructura objetiva de ese tipo penal.

BASES TEÓRICAS

Para lograr comprender la problemática planteada es necesario, clarificar los términos empleados, basados en conceptos, definiciones, fundamentos, teorías y principios que apoyan al esclarecimiento del objeto de estudio, en razón de lo anterior, se considerará importante revisar las nociones generales de los contratos electrónicos, sociedad anónima y sus delitos. Se comenzará con la línea de investigación de esta especialización

Sociedades Anónimas

Con respecto a la sociedad anónima venezolana también conocida como S.A, el Código de Comercio en el artículo 201 numeral 3, señala: “La compañía anónima, en la cual las obligaciones sociales están garantizadas por un capital determinado y en la que los socios no están obligados sino por el monto de su acción.”. Este concepto legal, destaca dos aspectos esenciales: primero, la de ser una sociedad de base capital, es decir tiene autonomía patrimonial, pues responden única y exclusivamente con sus bienes y segundo, la de limitar la responsabilidad de los socios por las deudas sociales hasta el monto de su acción, es decir que este tipo de sociedad, posee un patrimonio propio distinto de los sujetos que la integran.

Hacemos alusión a este término, por cuanto, esta investigación va dirigida a la actividad de contratar electrónicamente con este tipo de sociedad mercantil, los medios para que las mismas no sean víctimas ni incurran en fraudes u otro delito electrónico.

Doctrinariamente Acedo Mendoza y Acedo de Lepervanche (1991), consideran que la sociedad anónima:

“Es aquella sociedad constituida por personas cuya responsabilidad está limitada a los aportes que realizan para la consecución de un fin económico común, mediante la realización de actos de comercio; que tiene personalidad jurídica propia y distinta de la de los socios; que actúa bajo una denominación social, con un régimen legal de administración y cuyo capital está representado en acciones (p.106).

Por su parte, Barboza (2007) señala:

“La sociedad anónima está estructurada fundamentalmente sobre la base de un capital que los socios se obligan a integrar totalmente para que puedan constituir definitivamente la sociedad, por esta razón se afirma que es una sociedad de base capital constituida sobre el principio de intuitu rei no sobre el intuitu personae, al paso que esta compañía, una vez constituida lo determinante para su funcionamiento es el mantenimiento de su capital, no importando, por tanto, la consideración personal de los socios que la integran, pues éstos serán únicamente titulares de un documento denominado acción, que corresponde a una de las partes en que se ha dividido el capital, y será su tenencia la que determine ” (p.156)

Ambos autores, realizan dos características esenciales, vinculadas al capital social y la personalidad jurídica, esta última orientada a la realización del contrato social e inscripción de ese contrato en el Registro Mercantil del domicilio de la S.A. con su denominación social e inscripción en el registro de información fiscal (RIF), para que con ello la S.A. adquiera su condición de sujeto de derecho.

En este orden de ideas y con relación al capital social, es importante señalar que el Código de Comercio, no utiliza un criterio dimensional de capital social para la constitución de sociedades anónimas, en principio puede ser “cualquier cantidad”, sin embargo algunas leyes especiales, si exige un capital mínimo para ciertas empresas, por ejemplo: Los Bancos, entidades de ahorro y préstamo, empresas de seguro y reaseguro, entidades de inversión colectiva de capital abierto y cerrado, lo cierto es que actualmente el capital de la sociedad no puede ser insuficiente, debe tener por lo menos, un verdadero patrimonio, para desarrollar su objeto social y

responder por sus obligaciones, puesto que, frecuentes son los fraudes en especial los fiscales con sociedades anónimas de capital precario que sirven de simples instrumentos para grandes operaciones.

La cuestión dimensional del capital social, ha recibido solución legal, ahora con la Ley de Registro Público y Notariado vigente, específicamente en su artículo 56 numeral 1, que le atribuye la potestad al Registrador Mercantil de rechazar la inscripción de sociedades con capital insuficiente, aplicando criterios de razonabilidad relacionados con el objeto social y en opinión de esta investigadora, una Compañía Anónima con capital irrisorio estaría afectada de nulidad originaria, porque se encontraría en imposibilidad de cumplir con el objeto social, aunado a ello un capital insuficiente puede constituirse en un indicio de fraude.

El capital social de la compañía anónima está dividido en acciones y la responsabilidad de cada accionista está limitada al pago de las acciones que hubiere suscrito, los administradores de las mismas responden únicamente por su gestión y no por los negocios que realicen, sin embargo deben depositar en la caja social de la compañía un número de acciones como garantía de la ejecución de su mandato, para representar a la compañía se requiere la conformación de una Junta Directiva y para la toma de decisiones, es vital reunirse en asamblea de accionistas, ante estos preceptos, se puede caracterizar a la compañía anónima de la siguiente manera:

(a) Es una sociedad capitalista, porque en ella se destaca lo que los accionistas aportan a la sociedad y no sus cualidades personales, de tal manera que la participación de los accionistas y la distribución de los beneficios será de acuerdo a su aporte.

(b) Es una sociedad por acciones, es decir que la acción confiere a su titular de la condición de accionista y por ser la acción transferible, la integración humana puede variar, sin que ello conlleve cambios en la estructura social.

(c) Es una sociedad con limitación de la responsabilidad de los socios, la Ley dispone que el socio responde hasta por el monto de su acción, lo que significa que la responsabilidad de cada accionista está limitada al pago de las acciones que hubiere suscrito y las deudas de la sociedad no son deudas que afecte el patrimonio personal de los accionistas, el patrimonio separado se basa en la llamada autonomía patrimonial y personalidad jurídica.

(d) Es una sociedad gobernada por accionistas reunidos en asamblea, el órgano supremo de la S.A, es la asamblea, pueden ser ordinarias (que se realizan todos los años, al terminar el ejercicio económico) o extraordinarias (que son las que se realizan con ocasión a una eventualidad específica), el régimen se diseñó para ser democrático, sin embargo, en una sociedad, donde exista un accionista o grupo de accionistas mayoritarios, la mayoría predomina.

El en caso venezolano, la sociedad anónima, constituye el tipo societario de mayor relevancia en nuestra vida económica, pues su presencia se extiende a casi todas las actividades de producción de bienes y servicios, es el instrumento jurídico más adecuado para desarrollar empresas de gran amplitud, además permite la participación en ellas de un gran número de personas. Por tal razón, un instrumento jurídico de tal relevancia económica-social, requiere de vigilancia y control, así como, de regulaciones permanentes y actualizadas.

Comercio Electrónico

Según la Universidad de los Andes de Bogotá (2002) señala, por su parte, que el comercio electrónico (e-commerce) “se refiere a todas las transacciones comerciales realizadas o basadas en sistemas electrónicos de procesamiento y transmisión de información, especialmente EDI (*Electronic Data Interchange*) e Internet.” p.p 6-7. El desarrollo del comercio electrónico se inició con los instrumentos electrónicos siguientes: el teléfono, el fax, la televisión y los sistemas de pagos electrónicos, posteriormente, fue realizado a través de redes privadas como EDI, referida a la transmisión electrónica de datos de un computador a otro, estructurada bajo normas técnicas convenidas, su utilidad estaba relacionadas, con pedidos, cotizaciones, ordenes de compra e incluso facturación.

Posteriormente con la llegada de la Internet, el comercio electrónico se ha expandido significativamente y ha sido considerado como un elemento esencial para el crecimiento económico mundial, lo que conlleva gran importancia jurídica.

Definimos esta actividad por cuanto, de allí se desprende la contratación electrónica, por otra parte nuestro ordenamiento jurídico vigente, específicamente en la Ley para la Defensa de las Personas en el Acceso de Bienes y Servicios, se señala por primera vez, una definición de comercio electrónico, en los siguientes términos:

Artículo 30: A los fines de este decreto con rango, valor y fuerza de Ley, se entenderá como comercio electrónico, cualquier forma de negocio, transacción comercial o intercambio de información con fines comerciales, bancarios, seguros o cualquier otra relacionada, que sea ejecutada a través del uso de tecnologías de información y comunicación de cualquier naturaleza. Los alcances del presente Decreto con Rango, Valor y Fuerza de Ley, son aplicables al comercio

electrónico, entre la proveedora o proveedor y las personas, sin perjuicio de las leyes especiales.

Como se puede apreciar, esta disposición legal sirve de eje o soporte jurídico para la realización de toda actividad comercial por medios electrónicos, ya sea entre particulares, empresas y el mismo Estado, de igual manera, es importante destacar que la incorporación de esta definición en el ordenamiento jurídico Venezolano, es favorable ya que permitirá de manera significativa el establecimiento de mejores relaciones económicas internacionales, contribuyendo de esta manera al proceso de armonización que se está promoviendo internacionalmente en estas materias.

Contratación Electrónica

En cuanto a la Contratación Electrónica, Landáez (2009), afirma:

Se entiende por contratación electrónica aquella contratación que se realiza mediante la utilización de algún elemento electrónico, cuando este tiene, o puede tener, una incidencia real y directa sobre la formación de la voluntad o el desarrollo o interpretación futura del acuerdo. p. 155.

Igualmente, Del Carpio Narváez Luis (2009), presenta dos sentidos de la definición del contrato electrónico, así:

En sentido estricto, trata de aquellos contratos que se perfeccionan mediante un intercambio electrónico de datos de ordenador a ordenador. Frente a esta noción, existe una definición amplia, que incluye dentro de la categoría a todos aquellos contratos celebrados por medios electrónicos (aunque no sean ordenadores, como el fax, telex y teléfonos).

Una concepción muy similar a la anterior es descrita por la doctrina peruana, con el escritor Soto (2001), puesto que comparte la adición de que la definición de contratación electrónica tiene dos sentidos:

En sentido amplio, los contratos electrónicos son todos aquellos que se celebran por medios electrónicos, informáticos o telemáticos. En sentido estricto, son aquellos que se celebran mediante el llamado diálogo de computadoras, vale decir, entre el ordenador del emisor y el ordenador del receptor, a través de una red telemática binaria e interactiva de operadores intermedios.

En virtud de los aspectos que destacan estos dos últimos autores, definir el proceso de perfeccionamiento del contrato a través de un computador o un medio electrónico cualquiera, es un punto básico a tener en cuenta antes de comenzar la formación del mismo. Esta distinción es importante porque la selección de uno u otro implica la evaluación de diversos niveles de riesgo jurídico – tecnológico, al margen de lo anterior, en opinión de esta investigadora, se comparte, que la acepción estricta es muy conveniente para las empresas, más aún cuando se hagan en entornos cerrados como el EDI, ya que permitiría controlar posibles eventualidades difíciles de prever bajo un sistema abierto como lo es Internet, no obstante, Internet es la red de redes y no se puede desaprovechar la utilidad que comporta.

Es necesario destacar, que con estas definiciones se evidencia que el elemento informático se convierte en un medio esencial para la contratación, independientemente de su objeto y su celebración no hace necesario la presencia física y simultánea de las partes, en razón de lo anterior, se exhorta la reconsideración en el ordenamiento jurídico positivo vigente, sobre los conceptos tradicionales en materia de derecho de contratos, como ha sucedido cada vez que se han producido nuevos desarrollos tecnológicos.

Para una mejor comprensión de la contratación electrónica, se analizarán 3 principios sobre los cuales se basó la Ley sobre Mensaje de Datos y Firmas Electrónicas

Principios aplicados en la Ley sobre mensajes de datos y firmas electrónicas

Estos principios nacen con la Ley modelo para el comercio de UNCITRAL y su utilidad facilita el desarrollo legal y la armonización del comercio electrónico internacionalmente.

Principio de Neutralidad Tecnológica

Implica no favorecer unas tecnologías sobre otras ya que los estándares en esta materia deben ser impuestos por el mercado y no por ley, por tal motivo, La Ley sobre Mensajes de Datos y Firmas Electrónicas, mantiene el más estricto principio de neutralidad tecnológica con el fin de que permanezca vigente durante el mayor tiempo posible, es por ello que el primer aparte del artículo 1 dispone: "... El presente Decreto-Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro."

Con este artículo, el legislador intenta abarcar las tecnologías e innovaciones tecnológicas existentes y las que se establezcan en el futuro, para así evitar legislar sobre una determinada tecnología, esa intención fue reiterada al indicar en el título de la Ley, el término de firma electrónica y no el de firma digital que es más restrictivo, sin embargo, en opinión de algunos autores como Lozada (2010), señalan: "En el contexto jurídico ha sido difícil cumplir con esta normativa debido a que las normas que regulan la firma electrónica siguen como modelo y esquema la clave pública, basada en criptografía asimétrica". p 44

Esta concepción está vinculada con la legislación española y las disposiciones del Parlamento Europeo, puesto que en sus disposiciones expresan que sólo la firma electrónica basada en la actual tecnología - que es la de criptografía asimétrica – es comparable con los efectos de la firma manuscrita, situación que no es percibida expresamente en el caso venezolano, pues para que en Venezuela la firma electrónica tenga la misma validez y eficacia probatoria se requiere que cumpla con los requisitos del artículo 16 y 18 de la Ley de Mensajes de Datos y Firmas Electrónicas, mencionados más adelante, cabe significar que este artículo está vinculado con el principio de equivalencia funcional.

Principio de Equivalencia Funcional.

De acuerdo a la ley en comento, este principio se fundamenta en que estas nuevas denominaciones de carácter netamente tecnológico se equipare con sus similares del mundo físico, haciéndolas equivalentes sólo en lo que respecta a sus efectos y consecuencias, esta equivalencia funcional se da en la Ley principalmente entre las firmas electrónicas y firmas autógrafas y entre los documentos escritos y los mensajes de datos.

El legislador venezolano, ha incorporado el principio de equivalencia funcional en el artículo 4 y artículo 16 de la Ley sobre mensajes de datos y firmas electrónicas, al establecer: “artículo 4: Los Mensajes de Datos tendrán la misma eficacia probatoria que la ley le otorga a los documentos escritos...”. Este artículo permite aplicar a los mensajes de datos un principio de no discriminación respecto a las declaraciones de voluntad o manifestaciones de consentimiento y su incorporación al proceso judicial remite a las formas procedimentales reguladas para los medios de pruebas libres, previstas en el artículo 395 del Código de Procedimiento Civil

Artículo 16: La Firma Electrónica que permita vincular al signatario con el Mensaje de Datos y atribuir la autoría de éste tendrá la misma validez y eficacia probatoria que la Ley otorga a la firma autógrafa.

Este reconocimiento jurídico se complementa con que la firma este certificada por un proveedor de servicios de certificación electrónica y además este reconocimiento, se debe no sólo a su trascendencia en materia comercial, sino a otras materias como el caso del gobierno electrónico.

Principio de Autonomía de la Voluntad de las Partes.

Este principio se encuentra consagrado en la Exposición de Motivos de la Ley sobre mensajes de datos y firmas electrónicas. Es importante destacar que, la legislación venezolana, no obliga la utilización de la firma electrónica de la firma manuscrita, sino que su utilización es voluntaria.

Por su parte, Rico (2005), señala:

...implica fundamentalmente el respeto a la libertad de pacto, de modo que será siempre las partes las que decidan la forma como se van a llevar a cabo sus relaciones contractuales, considerándose de aplicación supletoria las normas legales, siempre y cuando esos pactos no afecten relaciones de orden publico. p.73

La autonomía de la voluntad de las partes y por tanto, la supletoriedad del régimen aplicable, se extiende también a la verificación, tanto de la emisión como de la oportunidad de emisión del mensaje de datos; a la determinación de los mecanismos para la recepción de los mensajes de datos; a la determinación del lugar de emisión y recepción del mensaje de datos, de donde deriva la jurisdicción y leyes aplicables en una relación jurídica y finalmente al acuse de recibo y mecanismos para verificarlo.

La consecuencia de la aplicación de estos principios es la no modificación del derecho, derivando así la naturaleza de ésta como una Ley Especial.

Teoría general de los contratos

En cuanto al extensivo, amplio y diverso contenido de esta teoría, analizaremos lo pertinente a los elementos para la existencia de los mismos, pero adaptado a los contratos electrónicos y para ello es pertinente, compartir lo señalado por, Salgueiro (2001), sucinto de la siguiente manera:

El Artículo 1.141 del Código Civil señala que “las condiciones requeridas para la existencia del contrato son: 1° Consentimiento de las partes; 2° Objeto que pueda ser materia de contrato; y 3° Causa lícita”.

Como se aprecia, la amplitud de la norma evidencia que no hay necesidad de una Ley previa que permita el cumplimiento de estos requisitos fundamentales por vía electrónica. Estos elementos esenciales del contrato, así como lo relativo a las fases de la contratación no presentan diferencias de fondo por el hecho de que la contratación se realice por vía electrónica. Las diferencias fundamentales entre la contratación tradicional y la electrónica se da por el medio a través del cual se manifiestan.

a) El Consentimiento

Es el fundamental y más delicado de los elementos de un contrato cualquiera sea su tipo, naturaleza o forma de perfeccionarse. El consentimiento es la manifestación de voluntad deliberada, consciente y libre que expresa el acuerdo de un sujeto de derecho respecto de un acto externo propio o ajeno.

La ley venezolana no presenta limitaciones en cuanto a la forma o medio de manifestación del consentimiento. La forma por excelencia de manifestar el consentimiento por vía electrónica es a través de un mensaje de datos.

Por lo anterior, se deduce que el uso de la informática como medio de expresión para la comunicación entre las personas es un medio válido para manifestar la voluntad y por tanto, un medio válido para contraer derechos y obligaciones, con o sin ley especial o general que lo admita o reconozca como tal. La forma por excelencia para identificarse electrónicamente son las firmas electrónicas. Salgueiro (2001), afirma:

El régimen establecido en la Ley para las firmas y certificados electrónicos de firmas es de carácter supletorio y solo es aplicable en caso que las partes no hayan acordado previamente un procedimiento alterno.

No obstante lo anterior, en las contrataciones electrónicas pueden existir vicios en el consentimiento y por el tema que se intentará exponer en esta investigación, como son los delitos en los contratos electrónicos, el vicio por excelencia es el dolo para el sujeto activo y el error para el sujeto pasivo en los casos de las defraudaciones informáticas, por tal motivo, es importante señalar, que esa relación jurídica contractual viciada, es nula, personalmente me inclino en estos dos vicios, como los que mayormente se incurre en este tipo de contratación, sin embargo, Pérez (2010), sostiene:

“En materia de contratación electrónica la mayoría de los casos guardan relación con el error como vicio de voluntad, ya que su ocurrencia es mucho mayor si la comparamos con los problemas que se puedan presentar con el fraude y la amenaza, es muy común incurrir en equivocaciones al utilizar equipos computacionales, muchas de las cuales se cometen de forma negligente o de manera no imputable, ya sea por una falta de conocimiento del usuario o simplemente por problemas técnicos. De esta manera el

consentimiento al manifestarse por medios electrónicos puede llegar a un destinatario distinto, en forma incompleta, o definitivamente no llegar sin que tenga conocimiento aquella persona que pretendía manifestar su voluntad. “.

La afirmación de esta autora es válida, sin embargo por el tema objeto de estudio, cuando se trata de delitos, los tres vicios (error, dolo y violencia) son posibles de aplicar las partes contratantes. Cabe señalar que la ley especial busca siempre la validez del contrato electrónico por ello establece que sus normas deben ser desarrolladas, interpretadas y orientadas a siempre reconocer la validez y eficacia probatoria de los Mensajes de datos y Firmas Electrónicas.

b) El Objeto

El objeto del contrato es la prestación, actividad o conducta que el deudor se compromete a realizar en beneficio de su acreedor. Pueden ser prestaciones o conductas de dar, de hacer o de no hacer, de medio o de resultado, puede consistir en la realización de una actividad o en la transmisión de un derecho. Según el artículo 1155 del Código Civil el objeto del contrato debe ser posible, lícito, determinado o determinable.

En contraposición con la contratación informática, en donde el objeto debe ser un servicio o bien informático, en la contratación electrónica, el objeto, no representa diferencia alguna. El objeto del contrato o convención electrónica debe cumplir las mismas condiciones establecidas en el señalado artículo 1155 ejusdem para su validez.

c) La Causa

La causa es la razón por la cual se ha realizado un contrato, el fin inmediato perseguido con la obligación contraída. Es un elemento subjetivo

muy discutido por la doctrina, sin embargo, el Código Civil hace breves referencias a la causa de los contratos. El artículo 1157 señala que la obligación sin causa, o fundada en una causa falsa o ilícita, no tiene ningún efecto y que la causa es ilícita cuando es contraria a la Ley, a las buenas costumbres o al orden público. El artículo 1158 señala que el contrato es válido aunque la causa no se exprese y que la causa se presume que existe mientras no se pruebe lo contrario.

Como se evidencia, la causa como elemento esencial de validez del contrato no se ve afectada por el hecho de que éste se celebre por vía electrónica.

La Firma Electrónica

La Ley Modelo de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional conocido por sus siglas UNICTRAL en su artículo 2, define la firma electrónica en general, como una conjunto de datos en forma electrónica, consignados en un mensaje de datos o adjuntados o lógicamente vinculados al mismo, que pueden ser utilizados para identificar el firmante de ese mensaje e indicar que éste aprueba la información allí contenida. Por su parte, en el artículo 2 de la Ley sobre Mensajes de Datos y Firmas Electrónicas, se encuentra su definición, como la “información creada o utilizada por el signatario, asociada al mensaje de datos, que permite atribuirle su autoría bajo el contexto en le cual ha sido empleado.” En definitiva el legislador venezolano reconoce el uso de la firma electrónica y le atribuye valor jurídico, pues un elemento indispensable en la prueba del contrato electrónico es que sea firmado electrónicamente ya que la firma por sí misma es capaz de asegurar aspectos que corresponden ser demostrados ante un Juez, como es la autenticidad e integridad del documento.

Sin embargo, para que la Firma electrónica sea considerada con plena validez y eficacia probatoria, además de estar debidamente certificada por un Proveedor de Servicios de Certificación Electrónica acreditados por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), deberá cumplir con los siguientes aspectos:

1. Garantizar que los datos utilizados para su generación puedan producirse sólo una vez y asegurar razonablemente su confidencialidad.
2. Ofrecer seguridad suficiente de que no pueda ser falsificada con la tecnología existente en cada momento.
3. No alterar la integridad del mensaje de datos.

Estos aspectos se encuentran regulados en el artículo 16 de la referida Ley y de no dar cumplimiento a estos requisitos unívocos y concurrentes, se constituirá la firma como un elemento de convicción valorable en Juicio, conforme a la regla de la Sana Crítica. La firma electrónica es defendible desde que las transacciones bancarias, los contratos, las compras, etc., se realizan on-line y para conseguir los mismos efectos de la firma manuscrita se requiere del uso de la criptografía y el empleo de algoritmos matemáticos específicos que claramente se explicará en el desarrollo de la presente investigación.

La Criptografía

Según Rico (2005). “La criptografía, del griego *graphos* (escritura) y *Kriptos* (oculto), es la ciencia que estudia la escritura secreta y la forma de ocultar el significado de la información. La criptografía se compone a su vez de dos ciencias específicas: la criptología, encargada de estudiar los procedimientos para cifrar y descifrar la

información y el criptoanálisis, que estudia la forma de esclarecer la escritura oculta.” p.188.

Para una mejor comprensión de lo señalado por esta autora, la criptografía es una rama de las matemáticas, que estudia los sistemas de cifrados, se complementa con el criptoanálisis, ya que, es la técnica de descifrar textos cifrados, es decir, realiza una especie de criptografía a la inversa y ambas ciencias (de cifrar y descifrar), forman la llamada criptología. En determinados casos y amparados mediante una orden judicial, existe la facultad, de que los Órganos de Investigación Penal, puedan acceder al contenido de un mensaje cifrado, mediante una operación de criptoanálisis y para ello se necesita un experto en la materia.

El Principio Básico de la criptografía es mantener la privacidad de la comunicación, entre personas, alterando el mensaje original de tal manera que sea incomprensible a personas distintas que el destinatario, es decir, su objetivo es impedir la interceptación de la información por terceras personas y en caso de lograrse, asegurar la incomprensión del mensaje. La criptología, con el tiempo se ha mantenido como una de las mejores técnicas criptográficas para la seguridad y confianza en redes abiertas como Internet y actualmente es el mecanismo más usado en los procesos de protección de datos, como son: correo electrónico cifrado, transacciones electrónicas bancarias y económicas, etc. Teniendo en cuenta que la naturaleza misma de Internet es la de ser un medio abierto y de libre acceso de información.

La Biometría

Según Torres (2005), define la biometría como “el medio tecnológico que tiene por objeto lograr la identificación de una persona, a partir de una o más de sus características fisiológicas.” p. 209

Esta definición recoge el principio de neutralidad tecnológica, en virtud de que incluye, toda tecnología que adecue cualquier característica fisiológica de una persona. Este hecho obedece a que la biometría puede asociar cualquier parte del cuerpo humano con una clave para verificar la identidad del usuario. Es el medio de seguridad para identificación de personas de mayor antigüedad, su funcionamiento se basa en la identificación y en la individualización de las personas, mediante sus rasgos fisiológicos, como son: el iris, las huellas digitales, reconocimiento facial, de la mano, entre otros. Para el autor Ruiz (2010), la aplicación de este sistema a través del iris es uno de los más altos de fiabilidad y más práctico en los reconocimientos biométricos y para demostrarlo comenta lo siguiente:

Este sistema de reconocimiento automatizado también se ha empezado a utilizar en el sistema bancario de algunos países, específicamente en los cajeros automáticos, donde el usuario es reconocido por el equipo y al insertar la tarjeta, procede a realizar la operación respectiva. P. 265

Los sistemas biométricos ofrecen la mejor de las garantías con respecto a la identificación de personas y su función en el comercio electrónico es garantizar la identidad de los sujetos que participan en él.

Teoría del Delito

Sin pretender abarcar de manera detallada, los diferentes aspectos contenidos en la teoría del delito, se hará una reseña de los elementos del delito y la teoría aplicada en el sistema judicial penal venezolano. Dentro del Derecho Penal, las posiciones doctrinales en la teoría del delito no son unánimes, por tal motivo resulta de gran dificultad obtener una definición única del delito, debido a la diversidad de escuelas penales, la variedad de criterios y la incertidumbre en cuanto métodos precisos y exactos,

históricamente se puede hablar de dos corrientes o líneas: la teoría causalista del delito y la teoría finalista del delito. Sin embargo, debe apuntarse que se tomará en consideración la Teoría Finalista del Delito cuyo defensor principal es el jurista y filósofo del derecho alemán Hans Welzel (1934), en virtud de ser la más aceptada universalmente y en Venezuela el propio Tribunal Supremo de Justicia la admitió totalmente, en sentencia de Sala Plena de fecha 04-06-2000 (Caso Miquilena), con ponencia del Magistrado Angulo Fontiveros. Esta teoría parte del postulado de que toda acción humana se ejecuta con una finalidad, es decir, es el ejercicio de una actividad final y no solamente causal como se describía en las teorías causalistas.

Para ampliar esta acepción, se refiere lo destacado por Velásquez (2002), al señalar:

El finalismo afirma que el legislador no es autónomo para erigir como delito cualquier comportamiento que le venga en gana, sino que tiene que respetar unos límites prejurídicos, y en ningún caso puede rebasar la dignidad de la persona humana como base mínima de cualquier convivencia civilizada. p. 218.

Lo que se destaca en esta afirmación, es que para que exista un delito deben concurrir varios elementos, pues la norma penal se crea y se interpreta para servir a la sociedad de lo contrario es atípico y de imposible aplicación, creando inseguridad jurídica.

Esta aseveración incidió de manera radical en los elementos del delito, tal y como lo señala el referido autor, así: en cuanto a la acción, presupuesto común a todas las formas de aparición del delito (dolosas o culposas), se concibe como ejercicio de actividad final y no solamente causal, entendiendo que esa finalidad se basa en la capacidad de previsión del hombre de las consecuencias posibles de su obrar.

En cuanto a la tipicidad, sufrió un vuelco muy grande en virtud de que si el contenido de la voluntad del agente se encuentra en la acción, está se ubica en la descripción concreta de la conducta prohibida, haciendo posible separar los delitos dolosos de los delitos imprudentes.

En cuanto a la antijuricidad, es entendida como aquella acción típica contraria a derecho, al orden jurídico, no protegida por causas de justificación y dependiente de algunos elementos subjetivos.

Por ultimo la culpabilidad, que es el juicio de reproche formulado al autor por no haber adaptado su conducta a la norma, a pesar de que estaba en situación de hacerlo.

En atención a las críticas de esta teoría, Reyes (1996), por su parte, sostiene:

En efecto lo que en este aspecto hizo Welzel, fue recoger las ideas filosóficas de Aristoteles y Santo Tomás de Aquino, en el sentido de que toda conducta humana es por esencia voluntaria y final, por manera que lejos de haberse inventado ese carácter final de la acción, lo que pretendió fue hacer valer dentro del Derecho Penal una característica inherente a la conducta humana: su intencionalidad. Por lo demás, los causalistas tampoco negaron nunca el carácter final de la acción humana sino que reconociéndolo, le otorgaron importancia sólo en el ámbito naturalístico y no en el jurídico como hiciera posteriormente el finalismo. p. 55.

No obstante lo anterior, se da a conocer una vez más la aplicación de esta teoría en el derecho actual y adaptado a las personas jurídicas, por tal motivo se hace referencia a una jurisprudencia de la Sala Constitucional del Tribunal Supremo de Justicia de la República Bolivariana de Venezuela, con ponencia de la Magistrada Carmen Zuleta de Merchán, Exp. 03-0296, Sent

Nº 834 de fecha 18-06-2009, relacionada con la responsabilidad penal de las personas jurídicas, donde establece:

la teoría de la adecuación típica se resuelve a través de la teoría de la imputación y no a través de la teoría de la relación causal; ubicándola en el plano valorativo y atendiendo a un concepto moderno y social de la acción, llamado también teoría objetivo-final de la acción. Según esta concepción los hechos o acciones deben concebirse como fenómenos naturales de la vida social y la responsabilidad penal debe ser entendida -en su función social- como atribución de pena de acuerdo a los parámetros constitucionales de protección preventiva de bienes jurídicos...

Tal postura, de cara a una concepción *laxa* de la responsabilidad penal, permite reorientar el concepto de imputación en la teoría del delito fracturando las estructuras ontológicas del Derecho Penal para concluir que las personas jurídicas ostentan la capacidad de culpabilidad penal -imputabilidad-, puesto que la culpabilidad ya no se concibe como un juicio de reproche eminentemente personal sino como un juicio que -en tanto función social- protege preventivamente los bienes jurídicos, siendo que la tutela penal abarca a todas las personas, ya sean estas naturales o jurídicas; aceptar lo contrario y aferrarse al principio tradicional *societas delinquere non potest* implicaría -frente a novedosas formas de criminalidad- dotar de impunidad a los entes colectivos y convertirlos así en gérmenes para la sociedad.

Como se pudo apreciar, indiscutiblemente hoy día se aplica esta teoría finalista a las sociedades anónimas que incurran en delitos y el elemento de culpabilidad es extensivo a personas jurídicas.

BASES LEGALES

Teniendo en cuenta la importancia que ha suscitado el comercio electrónico y el desarrollo de las nuevas tecnologías de la información en la dinámica comercial actual, haciendo mucho más operante la prestación de los servicios y el intercambio de bienes tangibles o intangibles, lo cual ha

resaltado la importancia de que nuestro país incorporara dentro de su estructura legal (se inicia a partir de 1999), normas que facilitaran las condiciones para acceder a canales eficientes de derecho mercantil internacional, con el propósito de reducir la incertidumbre causada por el uso de las nuevas herramientas tecnológicas en los ámbitos comerciales.

Constitución de la República Bolivariana de Venezuela.

En primer lugar señalaremos el llamado derecho de Habeas Data o el acceso a la información personal, principio consagrado en nuestra Carta Magna fundamental, contenida en su artículo 28, los cuales garantiza el derecho a las personas de buscar, recibir y difundir información, derecho íntimamente vinculado con el derecho a la libertad de expresión, la autonomía de la voluntad, respeto a la privacidad, honor, reputación, vida económica de las personas naturales y jurídicas etc.

Basta leer el artículo 28 de la vigente Constitución, para que todos estos derechos puedan identificarse. Dicha norma reza:

“Toda persona tiene derecho de acceder a la información y a los datos que sobre sí misma o sobre sus bienes consten en registros oficiales o privados, con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y a solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos. Igualmente, podrá acceder a documentos de cualquier naturaleza que contengan información cuyo conocimiento sea de interés para comunidades o grupos de personas. Queda a salvo el secreto de las fuentes de información periodística y de otras profesiones que determine la ley”.

Como se puede apreciar, aquí se consagra de manera expresa y por primera vez, la institución conocida como habeas data, la cual se solicita para obtener información sobre datos propios registrados, es decir, establece el derecho de las personas a conocer la información que sobre ellas, hayan sido compiladas por otras, este artículo tiene vinculación con el tema objeto de estudio, por cuanto, con el advenimiento de la Internet aumentaba las violaciones al derecho a la vida privada e identidad, no obstante este mecanismo, previene el cumplimiento del referido derecho.

Igualmente, la consagración constitucional del derecho al acceso a la tecnología, reconocido dentro de los derechos culturales en el art. 110 ejusdem, aunado al Plan Nacional de Telecomunicaciones del año 2000, implementado por la Comisión Nacional de Telecomunicaciones (CONATEL), donde se menciona la necesidad de incorporar a la Nación dentro de la Sociedad de la Información, establece entre los objetivos principales la promoción en el uso de las Tecnologías de Información y Comunicaciones, en el desarrollo productivo, se aprecia el propósito legislativo de lograr la actualización de las normas y la integración del país en el marco de una economía globalizada, que naturalmente permite las transacciones electrónicas.

Asimismo, consagra el derecho a la privacidad, en su artículo 48, al establecer:

Artículo 48: Se garantiza el secreto a la inviolabilidad de las comunicaciones privadas en todas sus formas. No podrán ser interferidas sino por orden de un Tribunal competente, con el cumplimiento de las disposiciones legales y preservándose el secreto de lo privado que no guarde relación con el correspondiente proceso.

En este sentido, la norma expresa que las comunicaciones privadas, son secretas, salvo que sean interceptadas por orden de un Tribunal, en razón de una investigación, por tal motivo, debe entenderse que los correos

electrónicos, las comunicaciones en vivo o videoconferencia, como medio para comunicarse, son privadas y están amparadas por la Ley

Código Civil Venezolano.

Asimismo tomando en consideración que en el acceso a Internet, el usuario ingresa al mismo libremente visitando distintos sitios, recabando información y pudiendo contratar, configurándose de esta forma el contrato electrónico, es menester señalar que en nuestro ordenamiento jurídico la contratación se rige por el principio de la Autonomía de la Voluntad, es por ello que en segundo lugar tenemos dentro de nuestro ordenamiento jurídico vigente el Código Civil Venezolano, Este principio, si bien no está consagrado explícitamente en nuestro Código Civil, surge de dos disposiciones legales a saber: la primera, del artículo 1.159 del Código Civil que establece “los contratos tienen fuerza de ley entre las partes...”; la segunda, del artículo 1.262 eiusdem que dispone que las obligaciones deben cumplirse exactamente como han sido contraídas; por tanto, de conformidad con las referidas disposiciones la ley permite la libertad contractual.

Código de Comercio Venezolano.

Este cuerpo legal, tiene como objeto regular las obligaciones de los comerciantes en sus operaciones mercantiles y los actos de comercio, el registro de comercio de los tipos de sociedades, las obligaciones de los contratos mercantiles en general, así como las compañías de comercio, de las cuales se analiza la regulación jurídica de las Sociedades Anónimas, considerado como el tipo societario de mayor utilidad en las empresas venezolanas, en el artículo 201, numeral 3, se encuentra la definición legal de las sociedades anónimas, explicado en las bases teóricas.

Código Penal Venezolano

Esta Ley General, tiene como objeto aplicar el principio de legalidad, se desarrollará analíticamente, el tipo de Estafa como uno de los delitos más comunes en las transacciones electrónicas, se encuentra tipificado en el artículo 462 y es del tenor siguiente:

Artículo 462. El que, con artificios o medios capaces de engañar o sorprender la buena fe de otro, induciéndole en error, procure para sí o para otro un provecho injusto con perjuicio ajeno, será penado con prisión de uno a cinco años. La pena será de dos a seis años si el delito se ha cometido:

1. En detrimento de una administración pública, de una entidad autónoma en que tenga interés el Estado o de un instituto de asistencia social.
2. Infundiendo en la persona ofendida el temor de un peligro imaginario o el erróneo convencimiento de que debe ejecutar una orden de la autoridad.

El que cometiere el delito previsto en este artículo, utilizando como medio de engaño un documento público falsificado o alterado, o emitiendo un cheque sin provisión de fondos, incurrirá en la pena correspondiente aumentada de un sexto a una tercera parte.

Decreto con Fuerza de Ley sobre Mensajes de Datos y Firmas Electrónicas y su Reglamento

Igualmente con este decreto Ley, que le otorga eficacia y valor jurídico a los mensajes de datos y firmas electrónicas, podemos apreciar que el contrato electrónico es reconocido por nuestro ordenamiento jurídico vigente al disponer en su objeto lo siguiente:

Artículo 1. El presente Decreto-Ley tiene por objeto otorgar reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

El presente Decreto-Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus

características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de Datos y Firmas Electrónicas.

La certificación a que se refiere el presente Decreto-Ley no excluye el cumplimiento de las formalidades de registro público o autenticación que, de conformidad con la ley, requieran determinados actos o negocios jurídicos.

Con este artículo, se logra constatar el aval normativo que se le ha dado a los desarrollos tecnológicos sobre seguridad en materia de comunicación y negocios electrónicos. La promulgación de este Decreto, tiene su origen en los trabajos de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (UNCITRAL), básicamente en los documentos elaborados por la Comisión sobre Comercio Electrónico: La Ley Modelo sobre Comercio Electrónico y la Ley Modelo sobre Firmas Electrónicas, instrumentos que crean el marco jurídico internacional a seguir, pues, tiene el cometido general de eliminar o reducir las disparidades en legislaciones nacionales que puedan crear obstáculos al comercio internacional en virtud de que su objeto es lograr la armonización de las distintas legislaciones en esta materia.

Ley Especial contra los delitos informáticos

Dicha Ley es promulgada con el objeto de proteger los sistemas que utilicen las tecnologías de la información, prevenir y sancionar los delitos que se cometan contra tales sistemas y sus componentes, o los contenidos mediante el uso de dichas tecnologías. Aún cuando esta Ley no regula en forma directa el comercio electrónico, conviene hacer referencia a ella, pues las actividades delictivas que se cometan a través de medios informáticos, dentro de las cuales se puede atentar en contra del comercio electrónico,

están sancionadas penalmente bajo el amparo de esta Ley. Se analizará específicamente el delito de oferta engañosa

Ley de Instituciones del Sector Bancario

Regula la actividad financiera, se vincula con la presente investigación, por cuanto, se analizará uno de los tipos penales aplicados a las transacciones electrónicas en las que intervengan este tipo de institución, como es el fraude electrónico.

Ley para la Defensa de las Personas en el Acceso de los bienes y servicios.

Este cuerpo legal, se vincula con el presente estudio en virtud de que establece por primera vez en Venezuela (cuando se denominaba Ley de Protección al Consumidor del año 2004), la regulación del comercio electrónico propiamente dicho, referida únicamente al comercio con consumidores, excluyendo las operaciones comerciales entre empresarios, exigiendo a los proveedores de bienes y servicios el deber de prestar atención a los intereses de los consumidores y actuar de acuerdo a las prácticas equitativas de comercio y publicidad.

Asimismo, prohíbe en forma expresa todo tipo de declaración falsa y engañosa, fraudulenta y discriminatoria por parte de los proveedores, acerca de los bienes y/o servicios que proveen, igualmente la restricción del uso de las comunicaciones comerciales no solicitadas, regula la naturaleza jurídica del contrato electrónico pues define y regula lo relacionado con los contratos de adhesión.

UNIDAD DE ANALISIS

Objetivos	Categorías	Indicadores	Instrumento	Fuente
Analizar exhaustivamente la regulación jurídica de la contratación electrónica para las sociedades anónimas en Venezuela.	Regulación Jurídica de la contratación electrónica para las sociedades anónimas en Venezuela	Naturaleza Jurídica Formación del Contrato (oferta y aceptación) Valor Probatorio del Documento Electrónico	Ficha contenido: Textual Resumen Mixta	de Doctrinas y leyes
Estudiar analíticamente los sistemas de seguridades en Internet para evitar los delitos en los contratos electrónicos.	Sistemas de Seguridad en Internet para evitar delitos en los contratos electrónicos	Firma Electrónica Criptografía Biometría	Fichas de contenido y matriz de análisis.	Doctrina y fuentes electrónicas.
Desarrollar de manera crítica los tipos penales aplicables a la contratación electrónica.	Tipos penales aplicables a la contratación electrónica	Oferta Engañosa Estafa Fraude Electrónico	Fichas de trabajo.	Leyes.

CAPITULO III

MARCO METODOLÓGICO

TIPO Y DISEÑO DE INVESTIGACIÓN

El presente estudio constituye una investigación documental, bajo un diseño de tipo descriptivo, en virtud que es apoyada en fuentes documentales, provenientes de obras literarias, paginas webs, trabajos de investigación, revistas, artículos de prensa, etc., material que será objeto de análisis.

Con respecto a la investigación documental, el manual de trabajos de grado de especialización y maestría y tesis doctorales de la Upel (2006), expresa:

Se entiende por Investigación Documental, el estudio de problemas con el propósito de ampliar y profundizar el conocimiento de su naturaleza, con apoyo, principalmente, en trabajos previos, información y datos divulgados, por medios impresos, audiovisuales o electrónicos. La originalidad del estudio se refleja en el enfoque, criterios, conceptualizaciones, reflexiones, conclusiones, recomendaciones y, en general, en el pensamiento del autor. p. 20.

Como se observa, este tipo de investigación depende de la información que se recoge o consulta en documentos, (entendiéndose éste en sentido amplio, como todo material de índole permanente), que conduce a la construcción de un nuevo conocimiento.

En términos generales el diseño de una investigación es la estructura a seguir en ella, ejerciendo el control de la misma a fin de encontrar resultados confiables y su relación con los interrogantes surgidos en el

problema, sin embargo es necesario definir, lo pertinente a diseño descriptivo y para ello se cita a Lerma (2004), quien señala: “La investigación descriptiva. Su objetivo es describir el estado, las características, factores y procedimiento presentes en los fenómenos y hechos que ocurren en forma natural, sin explicar las relaciones que se identifiquen.” p.64.

Es menester indicar que, con la designación descriptiva se recolectaron datos sobre aspectos, dimensiones y componentes para describir el contexto del fenómeno a investigar y así con el esquema del avance constitucional y legal con relación a los principios que conforman el tema estudiado, se compara el funcionamiento de las formas actuales señalando las principales características.

Recolección y selección de la investigación

Se emplearon varias técnicas y métodos de recolección de datos orientados a la consecución de los objetivos planteados en la presente investigación. Principalmente se empleó el análisis documental, que consiste en seleccionar las ideas relevantes de un documento a fin de expresar su contenido, sin ambigüedades para recuperar la información en él contenida. Esta representación puede ser utilizada para identificar el documento, para procurar los puntos de acceso e interés en la búsqueda de la información pertinente, para indicar su contenido o para servir de sustituto del documento.

Asimismo, se emplearon técnicas para el manejo de fuentes documentales como: el subrayado, citas y notas de referencia bibliográfica, de igual manera se registró, organizó y almacenó en la computadora información recabada por vía electrónica. De esta forma se logró organizar la información necesaria para el proceso de investigación, permitiendo así un

eficiente manejo de las fuentes bibliográficas. Entre los documentos que fueron sometidos a revisión, se encuentran: Trabajos relacionadas con las sociedades mercantiles como sujetos activos de delito en el comercio electrónico y contratos electrónicos, artículos de revistas electrónicas de derecho informático, también obras literarias impresas referente a los temas de interés que se demandaron.

Procedimientos de la investigación

En atención a esta modalidad de investigación, se procedió a cumplir con las siguientes etapas:

Primeramente, se seleccionó el tema y se estudió como punto de partida la Ley sobre mensajes de datos y firmas electrónicas, Código Civil, Ley contra los delitos informáticos, Ley para el Sector Bancario y el Código Penal, documentaciones jurídico-legales, con la descripción de los distintos puntos de vista doctrinarios que se han planteado los estudiosos en la materia, de manera que se pueda conseguir nuevos enfoques de la normativa en materia de contratación electrónica en el país.

Consecutivamente, se estableció la ejecución del trabajo de investigación que una vez elaborado y presentado, se impone su reestructuración cumpliendo y aplicando las pautas de la investigación jurídica, abarcando aspectos como son: la recolección, registro, clasificación, análisis, interpretación de los datos que ofrece la información, llevando así a las conclusiones o resultados que se relacionan con los objetivos propuestos.

Seguidamente, se tiene la comunicación de los resultados obtenidos en la investigación, a través del informe final, que permite el reconocimiento del trabajo realizado, el cual cumple con ciertos requerimientos relacionados con su contenido y presentación formal.

Con el razonamiento de las fuentes bibliográficas y electrónicas, se pudo comprender, describir y analizar la contratación electrónica y sus delitos en las sociedades anónimas de Venezuela, se consideraron las diversas fuentes formales y secundarias del derecho, relacionadas con el tema, como son: textos legales, doctrina nacional e internacional, es decir, las maneras de expresarse materialmente esta ciencia jurídica.

Se aplicó al lectura exploratoria, orientada a comprender en breve tiempo una idea integral de un escrito extenso, relacionar detalles y asegurar una síntesis a través de una comprensión general del tema.

En este estudio se realizó un resumen lógico del tema, el cual proyecta la comprensión del mismo, con las capacidades de razonamiento y habilidad creativa, con respecto a las referencias empleadas, fueron recolectadas en librerías, trabajos especiales de grado que reposan en la biblioteca del edificio de post-grado de la Ula-Mérida, investigaciones que existen en las bibliotecas virtuales de algunas Universidades y estudios que se encuentran en Internet.

Se aplicó el método de investigación documental, analítico-comparativa, entre las normas atinentes al tema objeto de estudio, mencionadas anteriormente, para relacionar la armonía existente en ellos, así como los vacíos legales que se puedan revelar.

Posteriormente, se procedió al ordenamiento del materia recabado, para irlo incorporando en todos los aspectos que se consideraron importantes, a través de las técnicas de estudio, recopilando toda la base teórica que sustenta esta investigación, se indagó sobre sus antecedentes, se construyó el contexto teórico para finalmente comprobar el problema que se planteó al inicio de la misma.

Se elaboró un marco teórico respaldado en diferentes artículos relacionados con el tema a desarrollar, se resuelve el problema, se efectúa el análisis crítico y se alcanzaron las respectivas conclusiones y recomendaciones.

www.bdigital.ula.ve

CAPITULO IV.

DESARROLLO Y DISCUSIÓN

El análisis e interpretación de la información recabada, se presenta siguiendo el desarrollo de los objetivos específicos planteados en esta investigación, de esta manera se agrupan los resultados, desde la siguiente perspectiva:

1. Analizar exhaustivamente la regulación jurídica de la contratación electrónica para las sociedades anónimas en Venezuela.

En el campo del Derecho, la manifestación de voluntad constituye un acto jurídico (bilateral o unilateral), destinado a producir un efecto jurídico, que por lo general se expresa a través de un soporte documental. Al trasladar esta situación al sistema electrónico viene a constituir una manifestación de voluntad más, pero instrumentada a través de medios electrónicos e igualmente destinado a un efecto jurídico. Por lo anterior, se quiere expresar que su validez y reconocimiento jurídico es igualmente análogo a los contratos tradicionales, pues, para el Derecho el contrato es un acto jurídico pero no todo acto jurídico es contrato, por ello es necesario primeramente reconocer lo indicado en el **artículo 1.133 del Código Civil Venezolano** al señalar que: “El contrato es una convención entre dos o más personas para constituir, reglar, transmitir, modificar o extinguir entre ellos un vínculo jurídico”.

Como se observa, el contrato es un esquema genérico, en el cual el elemento predominante es el consentimiento o acuerdo de voluntades, la legislación venezolana no presenta limitantes en cuanto a la forma o medio de manifestación del consentimiento, pues, todo acuerdo relativo a un objeto

de interés jurídico se convierte en contrato y es protegido por la Ley, sin embargo, en el caso de las contrataciones electrónicas la forma por excelencia de manifestar el consentimiento o voluntad, es a través del mensaje de datos, pues se equipara a un documento escrito, sin embargo, se debe tener especial cuidado con este elemento del contrato y para ello se debe implementar el mecanismo de la firma electrónica a fin de identificar el emisor del mensaje de dato e individualizar su consentimiento y evitar un futuro fraude en la contratación.

Para que una sociedad anónima se dedique a ofrecer bienes y servicios a través de Internet, se debe tomar en cuenta la normativa del Código Civil, Código de Comercio, Ley sobre Mensaje de Datos y Firmas Electrónicas y la Ley para la Defensa de las Personas en el Acceso a los Bienes y Servicios; contra cualquier hecho o publicación que constituya delito en la contratación por este medio corresponde la aplicación del Código Penal o cuando se realicen transacciones internacionales, el cual se vea involucrada más de una jurisdicción, se aplicarán los tratados internacionales a que haya lugar en cada caso particular. Igualmente cabe señalar, que cuando se trata de dirimir alguna controversia que se suscite con respecto a los actos de comercio, las partes quedan sometidas a la aplicación de la Ley Mercantil aunque el contrato sea mercantil para una de las partes, en virtud de la consecuencia en la individualización de los actos de comercio.

El Venezuela, al igual que en la mayoría de los países de América Latina se ha optado por crear una ley especial que amplíe todo lo relativo al la validez y eficacia probatoria de los medios electrónicos. Se trata del Decreto Ley sobre Mensaje de Datos y Firmas Electrónicas, ésta no es una ley de comercio electrónico ya que no tiene aspectos relacionados con el comercio en ninguna de sus formas, el objeto de este Decreto Ley, es el de otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje

de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material que pueda ser atribuida a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.

La elaboración de esta Ley establece en el artículo primero, que sus normas serán desarrolladas e interpretadas siempre en beneficio de la validez del documento electrónico y se basó en tres principios fundamentales de los cuales deriva una consecuencia que define la naturaleza de esta Ley, son ellos: la neutralidad tecnológica, la equivalencia funcional y el principio de autonomía de la voluntad de las partes; los cuales están descritos en las bases teóricas de esta investigación.

En razón de lo anterior, es necesario dilucidar la naturaleza jurídica del contrato electrónico y a su vez como se incorporan en él sus elementos:

1.1 Naturaleza Jurídica del Contrato Electrónico.

De acuerdo a las concepciones jurídicas establecidas en las bases teóricas, se puede afirmar, que el contrato electrónico es por lo general un Contrato de Adhesión, pues para formarlo se requiere la aceptación del vinculado, quien en caso de no estar de acuerdo podrá rechazarlo. Esta clase de contrato, es previamente redactado por una de las partes que generalmente, por su posición económica puede imponerle a la otra parte todas las estipulaciones del mismo, por ser ésta última, la parte débil de la relación contractual.

Su aparición nace inicialmente con los contratos relacionados con la prestación de servicios públicos (suministro de electricidad, agua, gas, etc.),

la empresa que suministra el servicio público está en capacidad de imponer todas las estipulaciones del contrato a quien requiere sus servicios, no hay conversaciones previas ni negociación, es importante destacar que esta clase de contratos no nace de la arbitrariedad de una de las partes, es consecuencia de la masificación de la prestación de un servicio o de la venta de bienes, inclusive de necesidad de técnica-jurídica y como se apreciará posteriormente una de las ventajas de las contrataciones electrónicas es la rapidez y masificación en el acceso de un mismo bien o servicio y por ello es apreciable que su formación sea de una realidad impuesta, motivada al orden económico y a la celeridad de las negociaciones.

La Ley para la Defensa de las Personas en el Acceso de Bienes y Servicios, destina un capítulo a los contratos de adhesión, comienza con su definición, exige que sean redactados en términos claros, específicos y en formato de fácil lectura para el consumidor, igualmente prohíbe la modificaciones unilaterales de las condiciones del contrato y en caso de hacerlo debe ser informado con un mes de antelación, señala el derecho del consumidor de retractarse por justa causa, finalmente establece unas estipulaciones para anular las llamadas cláusulas abusivas. Con respecto a la definición, señala:

Artículo 69. Se entenderá como contrato de adhesión, a los efectos de esta Ley, los contratos tipos o aquellos cuyas cláusulas han sido aprobadas por la autoridad competente por la materia o establecidas unilateralmente por la proveedora o el proveedor de bienes y servicios, sin que las personas puedan discutir o modificar substancialmente su contenido al momento de contratar.

En aquellos casos en que la proveedora o el proveedor de bienes y servicios unilateralmente establezcan las cláusulas del contrato de adhesión, la autoridad competente, podrá anular aquellas que pongan en desventaja o vulneren los derechos de las personas, mediante acto administrativo que será de estricto cumplimiento por parte de la proveedora o proveedores.”

Como se puede apreciar, en la definición de esta ley, se hace la distinción de la figura del contrato dirigido, que es cuando un órgano del Estado debe aprobar previamente las cláusulas del contrato, aquí la autonomía de la voluntad es limitada, por razones de orden público y equilibrio jurídico y uno de los ejemplos más frecuentes sucede con las pólizas de seguros que deben ser previamente aprobadas por la Superintendencia de Seguros.

Por su parte, Lozada (2009), sostiene que la naturaleza jurídica de los contratos electrónicos es en principio consensual, sin embargo en la actualidad pueden ser solemnes, debido a los efectos jurídicos deseados por las partes, no obstante, la solemnidad (en opinión de esta autora), es un requisito para su perfeccionamiento y hasta tanto en Venezuela, no existan los Registros Públicos virtuales, esa formalidad específica requiere de la presencia de las partes, lo cual se desvirtúa del contrato electrónico.

Además de lo anterior, es necesario destacar, que el contrato electrónico es un contrato entre personas lejanas o ausentes, pues se celebra entre personas que no se encuentran en el mismo lugar comunicándose entre sí, sino a través de mensajes de datos y para estudiar el proceso de formación del mismo, es preciso determinar el momento y el lugar en que se perfeccionó, atendiendo siempre al consentimiento de las partes contratantes.

1.2 Formación del Contrato Electrónico

El artículo 1.137 del Código Civil, señala que: “el contrato se forma tan pronto como el autor de la oferta tiene conocimiento de la aceptación de la otra parte”. Como se puede apreciar el proceso de formación del contrato no es otra cosa que la formación del consentimiento en sentido técnico,

igualmente se aprecia, que la legislación venezolana no presenta limitaciones en cuanto a la forma o medio de manifestación del consentimiento. La forma por excelencia de manifestar el consentimiento en un contrato electrónico es a través de un mensaje de datos y así lo reconoce jurídicamente el artículo 15 de la Ley sobre Mensaje de Datos y Firmas Electrónicas, el cual establece: “en la formación de los contratos, las partes podrán acordar que la oferta y la aceptación se realicen por medio de un mensaje de datos”. Ahora bien la armonía que caracteriza estos artículos es, que los contratos se forman por la integración de dos etapas sucesivas o casi simultáneas, que son: la oferta y la aceptación.

El análisis del perfeccionamiento del contrato, adquiere suma importancia, en virtud de que con ello se puede determinar cuando las partes pueden exigir el cumplimiento de las obligaciones contractuales. Existen 3 fases para la formación y ejecución del contrato, los cuales según Rico Mariliana (2005), se distinguen así:

- “*La fase de generación*, previa a la formación del contrato, referida al conjunto de actos que reflejan la intención de las partes de contratar, como sería la distribución y búsqueda de información, la selección del producto, o las comunicaciones previas entre las partes
- “*la fase de formación*, que coincide con el momento del perfeccionamiento del contrato, vinculando a las partes entre sí, dando origen a un negocio jurídico determinado, que tiene lugar cuando coinciden las manifestaciones de voluntad de los contratantes
- “*la fase de consumación*, durante la cual las partes cumplen con las prestaciones a que se han obligado por virtud del contrato.” p. 129

Con respecto a los contratos electrónicos, esta primera fase de generación pierde preeminencia, ya que, por ser su naturaleza jurídica un contrato de adhesión estas comunicaciones previas entre las partes no existen, (a menos que sean con el sistema EDI), sin embargo la intención de contratar se manifiesta a través del consentimiento de las partes que ha

pesar de no ser simultaneo, pues son contratos entre ausentes, requiere del concurso de la oferta y aceptación.

1.3 La Oferta y la Aceptación en los Contratos Electrónicos.

Preliminarmente, se debe observar que, para que el consentimiento expresado electrónicamente sea válido, las partes deben ser capaces, lo cual en materia de negocios electrónicos implica serias dificultades, teniendo en cuenta que las partes nunca están en presencia de la otra. Sin embargo en este caso las precauciones para que no se cometan defraudaciones estarán a cargo del proveedor de productos o servicios a través de la red, es decir, de la persona que a través de una pagina Web ofrece determinados bienes. También se debe rescatar que el objeto y la causa del contrato deben ser lícitos.

Para la formación del contrato se requiere que una de las partes tome la iniciativa y proponga al interesado el objeto, condiciones y modalidades del contrato que se quiere celebrar, así la otra persona puede manifestar su conformidad y de esta manera nace el vinculo contractual, estas etapas no son otras que la oferta y aceptación. En nuestra legislación nacional, el artículo 15 de la Ley sobre Mensaje de Datos y Firmas Electrónicas establece claramente que las partes podrán acordar que la oferta y aceptación se realicen por medio de mensaje de datos.

En lo que respecta a la oferta electrónica, tradicionalmente se define como una proposición unilateral que una de las partes dirige (a través del uso de las nuevas tecnologías de la información y comunicación) a la otra para celebrar con ella un contrato. No debe considerarse un acto preparatorio sino una declaración contractual, a través de la cual el contrato puede entenderse cerrado con la sola aceptación de la otra parte, sin necesidad de una ulterior

declaración del que hizo la oferta. La oferta debe ser completa, es decir, ha de contener todos los requisitos esenciales del contrato, para que pueda quedar perfeccionado con la sola aceptación del destinatario y ha de dar a conocer al destinatario la seria voluntad de obligarse del oferente.

En este mismo orden de ideas, Lozada (2009), identifica los requisitos de la oferta en cuatro literales, así:

- (a) Que sea completa, autosuficiente; debe contener todos los elementos del contrato propuesto, que permita que mediante la simple aceptación del destinatario se forme el contrato.
- (b) Contenga la intención de contratar; la intención del oferente de celebrar el contrato propuesto.
- (c) Debe ser conocida por el destinatario; que llegue a conocimiento de la persona a quien está dirigida.
- (d) Debe contener la determinación del oferente, es necesario que el destinatario de la oferta sepa con quien va a contratar es indispensable que el oferente se identifique, pero que el destinatario pueda comunicarle de manera precisa su aceptación así como brindar la seguridad del cumplimiento del contrato. En los contratos electrónicos, deberá contar con firma y certificados digitales. p.56

En este sentido, la oferta debe llenar los requisitos esenciales de un contrato, es decir, que por si misma tenga un contenido totalmente determinado de tal forma que la aceptación por parte del destinatario, conlleve el perfeccionamiento de un contrato, diferenciándose de lo que en la en la mayoría de las ocasiones constituyen mailing (mensajes con puros fines publicitarios), lo cual no pueden considerarse estos últimos verdaderas ofertas.

Las ofertas realizadas on line, en redes de comunicación como la Internet, se encuentra en forma permanente en las redes y las cuales se tiene acceso navegando por diferentes páginas, constituyen ofertas a personas indeterminadas. Los principales problemas que se presentan con

las ofertas incluidas en las paginas Web o transmitidas mediante e-mail, se centran en la dificultad de localizar el lugar de producción de la oferta y en el hecho de la determinación de la naturaleza jurídica de los mensajes contenidos en estos instrumentos, es decir, si realmente deben considerarse verdaderas ofertas que obliguen al oferente, o si por el contrario deben ser consideradas como simples mensajes publicitarios, ya que la oferta determina, el lugar donde se entiende celebrado el contrato, con las implicaciones jurídicas que esto conlleva.

En cuanto a la aceptación electrónica, es aquella declaración unilateral de voluntad que una persona realiza (a través del uso de las nuevas tecnologías de la información y comunicación), manifestando su asentimiento o conformidad a una propuesta recibida por ella, en los términos en que ha sido formulada aquella y de la manera requerida o autorizada por el oferente. Es decir, se exige la coincidencia total entre la oferta y la aceptación. Este requerimiento de la aceptación se denomina "regla del espejo", terminología empleada en la Convención de Viena de 1980, relacionado con el título El Contrato de Compraventa Internacional de Mercancías.

Al respecto, Lozada (2010), presenta los requisitos de la aceptación, son ellos: "(a) Debe ser congruente con la oferta. (b) Apertura, la aceptación debe ser hecha mientras la oferta se encuentre vigente. (c) Intención de contratar. (d) Que guarde la forma requerida." P. 58. De este contexto, se observa que la aceptación debe ser pura, es decir que se corresponda exactamente con la propuesta y en consecuencia forme el contrato.

Para Rincón C. Erick (2006), existen ciertas circunstancias o requisitos que son necesarios para que se forme el consentimiento y ellos son los siguientes: " (i) la aceptación debe darse mientras la oferta esté vigente; (ii) la

aceptación debe ser oportuna; (iii) la aceptación debe ser pura y simple.”
p.40.

Frente a la contratación a distancia o entre ausentes, el régimen aplicable a la contratación electrónica, se encuentra en diversas teorías de aceptación, este aspecto tiene especial relevancia, porque explican cual es el momento en que el contrato debe considerarse perfecto.

a) **Teoría de la declaración.** Para esta teoría, el contrato queda concluido en el momento en que el aceptante manifiesta que su voluntad coincide con la del oferente; por tanto, no hay necesidad de ningún otro acto para que se considere formado el contrato ni se requiere que la aceptación sea conocida por el oferente, tal celeridad es en ocasiones fundamental para la consecución de los propósitos perseguidos por el oferente, sin embargo no se sabe en que momento se acepta la oferta y la prueba judicial para determinarlo es muy difícil de allegar.

b) **Teoría de la expedición.** Para esta postura, el contrato no se forma con la sola manifestación de voluntad del aceptante, se requiere que la respuesta de ese aceptante sea enviada al oferente, con lo cual se deja en claro la intención inequívoca de obligarse. El acto de enviar la respuesta, señala el instante en que se forma el consentimiento. En este caso la correspondencia pertenece a su remitente, y éste puede retirarla antes de que llegue al destinatario y puede acontecer que el correo se extravíe, con lo cual el oferente quedaría en gran dificultad de probar que el destinatario ya había aprobado la oferta y por ende perfeccionado el contrato.

c) **Teoría de la recepción.** Esta teoría sostiene que el contrato queda concluido cuando la aceptación llega a la dirección del oferente, vale decir, cuando la aceptación se encuentra en el ámbito de interés del oferente, llegando la misma a su domicilio o establecimiento. Esta teoría ha obtenido

una gran acogida legislativa puesto que, con él es más fácil demostrar que la respuesta aprobatoria llegó, así como su contenido, sin embargo, en contraposición a esta aseveración, el jurista Maduro Luyando (2002), que denomina a esta teoría como fase o momento y la engloba dentro de la teoría de la concurrencia de las voluntades, señala que presenta un inconveniente práctico relacionado con la dificultad de probar cuando el oferente conoció efectivamente la aceptación, además expresa: “a esta teoría se le critica que retarda el momento del perfeccionamiento del contrato y que traslada los riesgos del perfeccionamiento al aceptante, cuando los debería correr el oferente, quien tomó la iniciativa de celebrar el contrato.” p.680

d) **Teoría de la cognición o conocimiento.**- Según esta teoría, el contrato es un acuerdo de declaraciones de voluntad, de modo que éste se considera concluido sólo cuando ambas partes conocen que la oferta ha sido aceptada, por tanto, el contrato se concluye cuando el oferente conoce de la aceptación de su oferta.

En el caso del ordenamiento jurídico venezolano, acoge la teoría del conocimiento en armonía con la teoría de la recepción, es decir, por una parte el código de comercio en el Art. 112 señala: “el contrato bilateral entre personas que residen en distintas plazas, *no es perfecto si la aceptación no llega a conocimiento del proponente...*” y por la otra, el enunciado del párrafo 1º del Art 1137 del Código Civil expresa: “el contrato se forma tan pronto como el autor de la oferta *tiene conocimiento* de la aceptación de la otra parte”. Ahora bien, ese conocimiento se presume que existe en el instante en que la aceptación llega a la dirección del oferente. Así lo dispone el párrafo 6º del citado artículo: “la oferta, la aceptación o la revocación por una cualquiera de las partes, *se presume conocidas desde el instante en que ellas llegan a la dirección del destinatario*, a menos que éste pruebe haberse hallado, sin su culpa, en la imposibilidad de conocerla.

Este reconocimiento contenido en el Art. 112 del Código de Comercio y párrafo 1º del Art. 1137 del Código Civil, es una clara aplicación a la teoría del conocimiento, pero el mismo Art. 1137 ejusdem, establece una presunción de conocimiento vinculada con la teoría de la recepción, sin embargo, es menester señalar que esta presunción es *juris tantum*, es decir, admite prueba en contrario.

Con relación a lo anteriormente expresado, es necesario mencionar que de conformidad con el Art. 13 de la Ley de Mensaje de Datos y Firmas Electrónicas y relacionándolo a la celebración de los contratos electrónicos, existe la posibilidad de condicionar la validez de la recepción del mensaje de datos a un acuse de recibo emitido por el destinatario, también las partes podrán establecer un lapso para la recepción del acuse de recibo y en caso de no haberse acordado, el mensaje de datos se tendrá por no emitido si el destinatario no envía su acuse de recibo en un plazo de 24 horas a partir de su emisión y si en efecto se recibe el mensaje de datos surtirá todos sus efectos.

Asimismo, respecto al lugar de la formación del contrato electrónico, es preciso indicar que el contrato se perfecciona en el momento y en el lugar en que el oferente adquiere efectivo conocimiento de la aceptación de su oferta por la contraparte y siguiendo las reglas sobre la emisión y recepción de los mensajes de datos contenidas en la Ley sobre Mensaje de Datos y Firmas Electrónicas, el Art. 12 establece: “Salvo prueba en contrario, el mensaje de datos se tendrá por emitido en el lugar donde el emisor tenga su domicilio y por recibido en el lugar donde el destinatario tenga el suyo”. Como se aprecia este artículo fija claramente la posición del lugar a ser considerado como origen de los datos o recepción de los mismos.

1.4 Valor Probatorio del Documento Electrónico

El documento electrónico como medio de prueba es atípico, sin embargo al representar la forma de expresar la voluntad de las partes, es admisible en virtud de principio de libertad probatoria y equivalencia funcional, ante este escenario, es prudente comenzar por reconocer la concepción amplia de documento.

Para el jurista colombiano Devis (1993), documento es: “toda cosa que sea producto de un acto humano, perceptible con los sentidos de la vista y el tacto, que sirve de prueba histórica indirecta y representativa de un hecho cualquiera” p. 486. Esa “toda cosa” se vincula a un corpus y se ha considerado como la base esencial o el ser mismo del documento. Según Pérez (2005), documento “es todo medio material donde se recojan manifestaciones de voluntad, se muestren imágenes representativas de un estado de cosas pasadas o se deje constancia de la ocurrencia de ciertos actos o hechos” p. 164. Vemos que ambos autores distinguen en sus definiciones los caracteres de: historicidad, esencia material y representatividad.

Dentro de las teorías sobre la naturaleza del documento se destacan la teoría del escrito y la teoría de la representación. Según la primera, el documento siempre es un escrito en algún soporte permanente o durable (tradicionalmente el papel). De conformidad con la teoría de la representación, el documento no es solamente un escrito sino todo objeto representativo o que pueda informar sobre un hecho o sobre otro objeto. Desde esta óptica el concepto de documento no está restringido a la naturaleza del soporte, ni a la forma escrita como único elemento material.

La teoría de la representación es aceptada por la legislación venezolana y se refleja claramente en el artículo 4 de la Ley del Mensajes de Datos y Firmas Electrónicas, al establecer, que los Mensajes de Datos

tendrán la misma eficacia probatoria que la ley le otorga a los documentos escritos.

La fusión de la informática y las nuevas técnicas de comunicación, así como la transferencia electrónica de datos, que permite intercambiar mensajes electrónicos en lugar de documentos escritos, son elementos del actual contexto digital que revalúan la concepción tradicional del documento y dan paso a los documentos electrónicos. El mensaje de datos es la esencia de los documentos electrónicos, la mencionada ley se refiere a éstos como “toda información inteligible en formato electrónico o similar que pueda ser almacenada o intercambiada por cualquier medio” (art. 2), e impone a los proveedores de servicios de certificación el deber de implementar los sistemas de seguridad para garantizar la conservación y archivo de los mismos.

Ahora bien, con base a lo anteriormente expuesto, se halló la siguiente definición de la Prof. Arias (2008), quien expresa que:

Documento electrónico es la representación idónea capaz de reproducir una manifestación de voluntad, materializada a través de las tecnologías de la información sobre soportes informáticos, que se expresa a través de mensajes digitalizados que requieren de maquinas para ser percibidos y comprendidos por el hombre.

Conforme a lo anterior, toda manifestación de voluntad, expresada en soportes lógicos y no físicos, que evidencie una obligación, puede ser considerada documento electrónico y la legislación vigente en materia de mensajes de datos si reconoce el valor probatorio de ese tipo de documentos y lo equipara al valor probatorio del documento escrito, estableciéndose en la misma legislación especificidades para la promoción, control, contradicción y evacuación de la prueba, y es que se realizará como medios de prueba libre como lo establece el Código de Procedimiento Civil.

Aún cuando La prueba por escrito se encuentra regulada en los artículos 1.355 y siguientes del Código Civil y en los artículos 429 y siguientes del Código de Procedimiento Civil, las mismas no prevén los documentos electrónicos, sin embargo no impide la utilización de estos tipos de medios probatorios y los artículos 1355 del Código Civil y 395 del Código de Procedimiento Civil, deja la posibilidad de incorporarlos, pues no los prohíbe expresamente. De cualquier modo, al corroborarse su autenticidad en el reconocimiento judicial, tal como lo establecen las reglas de procedimiento y valoración previstos para la prueba por escrito, entonces ¿porqué no podría ser admitida como prueba documental?.

Al respecto, Arias (2008), al analizar una sentencia del Tribunal Supremo de Justicia de la República Bolivariana de Venezuela, de fecha: 12 de febrero de 2008, explica la naturaleza de esta situación jurídica al expresar:

La valoración de la prueba, ésta queda sometida a la libre apreciación del juez. El problema radica que, en condiciones normales, los contratos electrónicos contenidos en soportes informáticos, podrían ser vulnerados por las partes; dicha vulnerabilidad debe ser eliminada mediante la implementación de tecnologías (firma electrónica) que lo permitan y de la intervención de terceros confiables. Esto llevaría a la consecución de un valor probatorio análogo al de los documentos escritos en soporte papel. p. 186

Como se aprecia lo descrito por esta autora tiene su razón de ser, pero también es importante resaltar que en ese año la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), no estaba en funcionamiento, por tal motivo, las firmas electrónicas contenidas en los mensajes de datos no generaban certeza jurídica en su forma y contenido. Pero como tal situación en la actualidad ya está siendo controlada por el ente

mencionado y en virtud del principio de equivalencia funcional, se crea la convicción de que los Documentos Electrónicos y las Firmas Electrónicas que utilicen un certificado emitido por un Proveedor de Servicios de Certificación Electrónica acreditado por la SUSCERTE, tendrán la misma eficacia y validez del documento escrito y la firma manuscrita respectivamente, en consecuencia si pudieran ser valoradas como pruebas documentales propiamente dichas.

2. Estudiar analíticamente los sistemas de seguridad en Internet para evitar delitos en los contratos electrónicos

Actualmente las empresas que ofertan sus productos a través de Internet, no obtienen las ganancias necesarias para subsistir únicamente del comercio electrónico. La mayoría de estas empresas realizan contratos tradicionales y utiliza el contrato electrónico, para obtener mayores ganancias. Ello, porque los usuarios dudan al ingresar información que pueda ser atraída por un pirata informático. Por ejemplo, luego de adquirir un bien o servicio se realiza el pago respectivo, para ello el comprador deberá ingresar el número de su tarjeta de crédito o débito, sin saber si existe la seguridad de que esa información no será mal utilizada ni obtenida por un tercero de mala fe.

Motivado a lo anterior, la necesidad de generar confianza y proteger el derecho del consumidor a la privacidad de sus transacciones permitirá el mayor desarrollo del comercio electrónico en la modalidad empresa - consumidor. Este propósito está vinculado con que los mecanismos de transacción sean accesibles, seguros y legales para que así tanto las empresas como los consumidores recurran a esta nueva forma de contratar.

Para proponer esa confianza al consumidor se utilizan sistemas de seguridad que codifican el mensaje enviado, de manera que si el mensaje es

captado por un tercero, éste no podrá descifrarlo, en este capítulo se explicarán algunos sistemas de seguridad en Internet que ayudan a la prevención de conductas delictivas fraudulentas, son ellos:

2.1 La Criptografía

Toda encriptación se encuentra fundamentada en algoritmos, que codifican la información para que sea indescifrable y no se pueda interpretar con verlo, actualmente los sistemas criptográficos se basan y están vigilados en las claves de encriptación (llaves), que son operaciones matemáticas muy complejas y determina la manera en que la transformación del mensaje es realizada, estos sistemas criptográficos pueden ser de dos clases:

Sistemas de cifrado simétrico, clave privada o encriptación tradicional.

Consiste en utilizar la misma clave para el cifrado y el descifrado, es decir, cada dueño de usuarios que desee enviarse un mensaje debe tener una clave secreta, sólo conocida por ambos, puesto que, es misión fundamental tanto del emisor como del receptor conocer esta clave y mantenerla en secreto.

Como sustento de lo anterior, Rico (2005), afirma: "La autenticidad de los mensajes, se consigue siempre y cuando los usuarios mantengan la clave en secreto." p.191. La autenticación que señala esta autora, es el proceso que comprueba y verifica la identidad de una persona que se conecta al sistema, lo cual supone que si la llave cae en manos de terceros, el sistema deja de ser seguro, por lo que habría que descartar dicha llave y crear una nueva.

En los sitios donde existe un número limitado de usuarios y un gran volumen de información, la criptografía de llave simétrica es efectiva, sin

embargo, en redes grandes con usuarios distribuidos en un área amplia la repartición de las llaves se convierte en un problema, puesto que, es peligroso que muchas personas deban conocer una misma clave, además es difícil almacenar y proteger cuantiosas claves diferentes que son necesarias cuando hay bastantes usuarios, ya que, cada uno de los individuos en una red debe tener una llave diferente para comunicarse con cualquier otro usuario, por ejemplo: Un sistema de 1.000 usuarios, requeriría aproximadamente de 500 llaves para ser intercambiadas y mantenidas de manera segura.

Entre los algoritmos de encriptación o cifrado de clave simétrica, se encuentran los sistemas: DES, Triple DES y RC5.

- **Sistemas de Cifrado DES (Data Encryption Standard):**

Es un algoritmo de encriptación que se utiliza como método para cifrar información, su uso se ha propagado ampliamente por todo el mundo, como lo indica Moreno (2002): “DES es un esquema de encriptación simétrico desarrollado en 1977 por el Departamento de Comercio y la Oficina Nacional de Estándares de EE.UU. en colaboración con la empresa IBM, que se creó con el objeto de proporcionar al público en general un algoritmo de cifrado normalizado para redes de ordenadores”. Se utilizó rápidamente para ofrecer confidencialidad en aplicaciones gubernamentales y para garantizar la integridad en la industria financiera.

Para explicar su funcionamiento, Moreno expresa:

Se Basa en un sistema monoalfabetico, con un algoritmo de cifrado consistente en la aplicación repetida de varias permutaciones y sustituciones. Inicialmente el texto a cifrar se somete a una permutación, con bloque de entrada de 64 bits, para posteriormente ser sometido a la acción de dos funciones principales, una función de

permutación con entrada de 8 bits y otra de sustitución con entrada de 5 bits., en un proceso que consta de 16 etapas de cifrado.

Aunque este sistema presenta los riesgos, explicados al comienzo anterior, este sistema es ventajoso por su simplicidad y fácil implementación ya sea basado en hardware y en software.

En la actualidad es considerado un secreto nacional de EE.UU., por lo que está protegido por leyes específicas, y no se puede comercializar ni en hardware ni en software sin el previo permiso específico del departamento de Estado; también, su clave es corta lo cual no asegura una fuerza adecuada, por lo que con la potencia venidera de los computadores y con el trabajo en equipo por Internet se cree que puede violar el algoritmo, ha ocurrido, volviéndose inseguro para propósitos de alta seguridad

No obstante, algunos expertos utilizan este sistema para explorar nuevas técnicas de criptoanálisis, y aun no hay técnica criptoanalítica que puedan quebrar completamente a Des de una manera estructurada, siendo la única debilidad conocida en pequeño tamaño de su clave. Para solucionar el problema de longitud de clave, se comenzó a implementar el Triple DES, que no es más que un triple cifrado basado en DES.

- **Sistema de Cifrado Triple DES:**

Muchos de los anteriores usuarios de DES, ahora utilizan Triple DES, también llamado TDes o Des Multiple, que fue descrito y analizado por una de las patentes de DES y consiste en la aplicación de DES tres veces consecutivas, empleando tres claves, normalmente es una secuencia de encriptación-desencriptación-encriptación con tres llaves diferentes y sin relación entre ellas, hasta ahora este sistema ha sido ampliamente reconocido como seguro, aunque es bastante lento, este algoritmo toma una clave de 128 bits. y la divide en dos de 64 bits. cada una, es decir, se le

aplica al documento a cifrar un primer cifrado mediante la primera clave C1, al resultado (denominado ANTIDES) se le aplica un segundo cifrado con la segunda clave, C2. y al resultado se le vuelve a aplicar un tercer cifrado con la primera clave C1.

En opinión de Angel:

“En los últimos 20 años se han diseñado una gran cantidad de sistemas criptográficos simétricos, entre algunos de ellos están: RC-5, IDEA, FEAL, LOKI'91, DESX, Blowfish, CAST, GOST, etcetera. Sin embargo no han tenido el alcance de DES, a pesar de que algunos de ellos tienen mejores propiedades.

Podemos afirmar que el estado actual de la criptografía simétrica es la búsqueda de un nuevo sistema que pueda reemplazar a DES en la mayor parte de aplicaciones. Es así como se ha optado por convocar a un concurso de sistemas criptográficos simétricos y que este decida quien será el nuevo estándar al menos para los próximos 20 años. p.14.

Estos llamados de concursos que señala Angel, se perciben desde el año 1998, llegando en el año 2000 cinco finalistas MARS, RC-6, Serpent y TwoFish y Rijndael, sin embargo, hasta ahora Tdes tiene consideraciones específicas como Des, puesto que juegan un rol fundamental en la construcción de una criptografía fuerte para el público.

- **Sistema de Cifrado RC5**

Este algoritmo de cifrado fue desarrollado por Ron Rivest de la empresa RSA Data Security Inc. Una de las más importantes en el campo de los sistemas de cifrados y protección de datos, dicho algoritmo, se dio a conocer en el año 1995, es el sucesor de RC4 y hace uso de tres parámetros diferentes para operar, es decir, cifra mensajes de 32, 64 y 128 bits, es ampliamente configurable, permitiendo fijar diferentes longitudes de clave, número de interacciones y tamaños de los bloques a cifrar, por lo que

permite adaptarse a cualquier explicación, este algoritmo es el usado por Netscape para implementar su sistemas de seguridad en comunicaciones.

El RC5, utiliza computación básica y operaciones que comúnmente se encuentran en microprocesadores, por lo que es adecuado para ser implementado en hardware y en software, es rápido y sencillo, además permite diferentes longitudes de clave aunque está prohibida su exportación fuera de EE.UU. con longitudes superiores a 56 bits. longitud considerada corta por los cirptoanalistas, situación que hace sospechar que RC5 no es lo suficientemente seguro.

Como señala, Moreno “Las principales desventajas de los métodos simétricos son la distribución de las claves, el peligro de que muchas personas deban conocer una misma clave y la dificultad de almacenar y proteger muchas claves diferentes”.

Sistemas de cifrado asimétrico o de clave publica

Estos sistemas criptográficos, utilizan un par de claves complementarias: mediante una de ellas se realiza el cifrado y la segunda se emplea para descifrar el mensaje, es decir, una de las claves se mantiene secreta y la otra se hace pública. Si ocurriere el caso de que una de las claves se divulgue, no complica la seguridad de la comunicación, porque es imposible determinar la clave privada a partir de la pública.

Los sistemas criptográficos pueden utilizarse de dos (2) modos en función de si la clave publica se usa como clave de cifrado o de descifrado. En el primer caso, el modo de operación se denomina modo de cifrado y, en el segundo, modo de autenticación.

En el modo cifrado: La clave pública se utiliza como clave de cifrado, por ejemplo; garantiza la confidencialidad de un mensaje. Su base de

funcionamiento es la siguiente: las claves públicas de todos los usuarios se almacenan en un directorio. Como estas claves publicas se emplean como claves de cifrado, cualquier usuario que desee enviar un mensaje confidencial a otro usuario simplemente busca la clave publica del destinatario en el directorio y la utiliza para cifrar el mensaje que desea transmitirle. Por último, solo el poseedor de la clave privada asociada puede descifrar el mensaje y leerlo, con lo cual se asegura la deseada confidencialidad.

En el modo de autenticación: utilizar la clave pública para descifrar un mensaje permite verificar la identidad del emisor y comprobar la integridad del mensaje (autenticación del mensaje). A cualquiera que posea la clave pública le es posible descifrar y leer el mensaje, pero sólo el poseedor de la clave privada esta capacitado para generar el mensaje cifrado. Este método de encriptación se utiliza para la firma electrónica (que explicaremos mas adelante).

Estos métodos facilitan la gestión de las claves, ya que se elimina la necesidad de almacenar un número universal de claves, permitiendo, que estas sean distribuidas a través de sistemas no protegidos, como por ejemplo: Servicios de directorio. Sin embargo, este sistema presenta algunos riesgos que fueron inmediatamente remediados y Rico (2005), lo explica así:

El mayor inconveniente que se puso de manifiesto cuando comenzaron a utilizarse los sistemas asimétricos radicaba en la vinculación de una persona con un par de claves, ya que cualquiera, aún firmando el mensaje, podía negar que había usado una firma basada en una clave determinada al no estar vinculada a un sujeto específico. Para solucionar esta situación, se ideó la intervención de una tercera parte- el prestador de servicios de certificación- encargada de certificar que una clave publica se corresponde con una clave privada determinada y que estas pertenecen a una persona específica, función que se cumple a través de la emisión de certificados electrónicos. p.p 272 al 273.

La implementación más exitosa de un sistema de criptografía de clave publica es el algoritmo **RSA** (utilizado por SSL, Firma Digital y SET, secure electronic Transfer Protocol) creado en 1978, cuyas iniciales son por sus creadores: Rivest, Shamir y Adleman. Es método de cifrado se basa en el hecho de que, aunque encontrar números primos grandes es relativamente fácil, factorizar el producto de tales números, se considera actualmente imposible. Como lo señala España (2003), "El sistema RSA se ha mostrado durante años resistente a sucesivos intentos por parte de expertos de desbancarlo, siendo valorado actualmente como uno de los sistemas de cifrado conocidos más seguros". p.61

Como se aprecia este sistema es muy ventajoso, por su seguridad y empleo de claves, sin embargo presenta el mismo inconveniente de los cifrados simétricos y es su lentitud, por tal motivo, los expertos en criptografía, recomiendan el empleo de ambos sistemas (simétrico y asimétrico), para que su funcionamiento sea el ideal.

El protocolo SSL (Secure Sockets Layer),

Asegura la comunicación bidireccional, fue iniciada por Netscape luego por otros servidores y navegadores web, convirtiéndose en el más popular en Internet, utiliza temas de cifrado simétrico y asimétrico, esta conexión es iniciada por un usuario que con el propósito de acceder a un navegador que reconozca SSL, bastaría con reemplazar http por "https", de esta forma obtendrá información segura, para ello se requiere identificar el icono de un candado dorado que si aparece cerrado indica que la pagina fue descargada con SSL y es segura, de esta manera se proporciona un canal de comunicación seguro entre servidores web y usuarios.

Con la implementación de ambos sistemas (simetrico y asimetrico), podemos apreciar lo que proporciona este protocolo, Rico (2005), señala: "El

cifrado de la información, la autenticación de los servidores, la integridad del mensaje y opcionalmente la autenticación del cliente, pero no proporciona la confidencialidad, y el no repudio del mensaje..”.p. 216.

Quiere decir que, este protocolo sólo garantiza la confidencialidad e integridad de los datos en tránsito mientras viajan entre el usuario (navegador) y servidor, es decir, es un protocolo seguro de propósito general, sin embargo, no fue diseñado para las transacciones electrónicas comerciales, puesto que, no verifica la validez del número de tarjeta recibido, ni procesa la transacción con el banco del usuario cliente, para ello se creó el Protocolo Set.

El Protocolo Set.

Fue el sistema de seguridad que desarrollaron las empresas Visa y Master Card, con la colaboración de otras compañías como IBM, RSA, Netscape, Microsoft, entre otros, posee una billetera electrónica, un servidor y un servicio de pagos Set, el procedimiento para utilizar este sistema lo explica, Domingo (2004), al expresar:

El usuario introduce su número de tarjeta de crédito en el software de billetera electrónica, el cual se almacena encriptado en el disco duro; se crea también una llave pública y una privada para encriptar la información financiera antes de enviarla a través de Internet. Cuando un usuario desea comprar algo, su número de tarjeta de crédito es enviado encriptado al comerciante quien firma digitalmente el mensaje de pago y lo envía al banco, donde el servidor de pagos desencripta la información y realiza el cargo a la tarjeta. p.67

Este protocolo sólo cifra el número de tarjeta de crédito que ni siquiera el comerciante llega a verlo y así evitar fraudes, además se cerciora que la información no sea alterada de manera accidental o intencional mientras viaja en la red, para ello requiere de algoritmos de firma electrónica.

Es importante destacar que, aunque los sistemas de clave pública mejoran rotundamente la gestión de las claves, puesto que, estas pueden ser de dominio público y la clave privada siempre está oculta y en dominio de su propietario, estos algoritmos dificultan la implementación del sistema, por lo que son considerados por expertos como lentos si se comparan con los sistemas simétricos. Por el contrario, mientras que los sistemas simétricos permiten el cifrado eficiente de mensajes extensos, requieren un acuerdo previo en las claves y poseen capacidades de autenticación limitadas.

Indudablemente los sistemas de cifrados son una herramienta que aumenta la seguridad en las comunicaciones, sin embargo tienen un dato comprometido y es que esconden virus a los antivirus perimetrales insuficientes, puesto que si el emisor cifra un mensaje también cifra el virus y ningún antivirus puede descifrar el mensaje para su análisis de virus, en este caso, lo recomendable es brindar una protección segura que bloquee elementos cifrados no autorizados antes de que alcancen los servidores y las estaciones de trabajo.

2.2 La Firma Electrónica

La firma electrónica se vincula con la criptografía, por cuanto está fundamentada en un esquema de seguridad basado en esta ciencia, utilizando el método de encriptación de clave pública, es decir, es un conjunto de caracteres que se obtiene como resultado de someter el mensaje a una función matemática, estos caracteres se adicionan al mensaje y se envían encriptadas con la clave privada del emisor, cuando el destinatario lo recibe somete el mensaje a la misma función matemática (denominado función hash), posteriormente abre el mensaje encriptado que contiene los caracteres, con la clave pública del emisor (denominado hash result). Finalmente, si al comparar los caracteres enviados y el resultado obtenido al

someter el mensaje a la misma función matemática, resultan idénticos, el mensaje que envió el emisor no fue interceptado ni leído por un tercero. La función matemática es muy sensible y en caso de que se haya modificado en algo el mensaje, por leve que sea la modificación, el resultado será distinto. También se asegura de esta manera que el resultado de caracteres sea único y no habrá dos iguales.

Este procedimiento otorga autenticidad y brinda seguridad e integridad al mensaje. La Seguridad e Integridad se obtiene del uso de la criptografía, que es un mecanismo utilizado para enviar mensajes, sin que nadie distinto al destinatario pueda descifrarlo. Esta tecnología consta de 2 claves, una privada y una pública, que se asigna a una misma persona. El emisor encripta el mensaje con la clave Pública del destinatario, que es conocida públicamente, y el destinatario desencripta el mensaje con su clave privada.

Para saber que la clave pública del destinatario es la que dice ser, es necesario que exista una autoridad de certificación, en el caso venezolano los que proporcionan, revocan o suspenden los distintos tipos o clases de certificados electrónicos son los Proveedores de Servicios de Certificación, acreditados por la Superintendencia de Servicios de Certificación Electrónica.

El Certificado Electrónico, garantiza la autoría de la firma electrónica que certifica así como la integridad en el mensaje de datos, tiene un período de vigencia determinado de mutuo acuerdo entre el Proveedor de Servicios de Certificación Electrónica y el Signatario, sin embargo puede ser objeto de cancelación o suspensión temporal a solicitud del signatario, no eximiéndolo de las obligaciones y responsabilidades contraídas durante la vigencia del certificado y están regulados en el capítulo VII de la Ley sobre Mensajes de Datos y Firmas Electrónicas.

Los Proveedores de Servicios de Certificación Electrónica, son personas naturales o jurídicas, con suficiente capacidad económica, financiera y técnica para prestar los servicios autorizados como proveedor (Entre ellos la expedición de certificados electrónicos) con sólidos planes y procedimientos de seguridad en los sistemas e instalaciones físicas de manera que garantice la prestación continua de los servicios, actividades y cumplimiento de obligaciones, estipuladas en el capítulo VI de la referida Ley, pueden tener naturaleza pública o privada y para prestar servicios en Venezuela, requieren ser acreditados por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE).

Actualmente existen sólo dos (02) empresas acreditadas por SUSCERTE para la emisión de certificados electrónicos, una empresa pública, denominada Fundación Instituto de Ingeniería para Investigación y Desarrollo Tecnológico (PSC-FII), acreditada desde el año 2008 y ofrece sus servicios a empresas públicas y organismos gubernamentales, entre otros y una empresa privada, denominada Proveedor de Certificados (PROCERT C.A), su aliado tecnológico es la empresa Whisekey, proveedora de Servicios de Certificación en el mercado europeo.

La Superintendencia de Servicios de Certificación Electrónica, es un Organismo autónomo adscrito al Ministerio del Poder Popular para la Ciencia y Tecnología, el cual tiene por objeto acreditar, supervisar y controlar, en los términos previstos en la Ley sobre Mensajes de Datos y Firmas Electrónicas y su Reglamento a los Proveedores de Servicio de Certificación Electrónica, tanto públicos como privados, Las competencias, están establecidas en el artículo 22 de la Ley sobre Mensajes de Datos y Firmas Electrónicas.

Las aplicaciones y manifestaciones más importantes de la criptografía, se están desarrollando con la firma electrónica, permitiendo que las transacciones económicas sean confiables, sin embargo, este componente

tan importante para el comercio de bienes y servicios vía electrónica, requiere de una amplia regulación, y de allí se comparte la afirmación de Díaz (2008) al señalar la necesidad de introducir reformas desde el punto de vista penal para la regulación de la firma electrónica y de allí propone agregar elementos claves para su incorporación como objeto de delito, ante ello, la referida autora afirma:

...aun cuando en Venezuela, se adoptan algunas sanciones en materia de comercio electrónico, las mismas en ningún momento están relacionadas con la firma electrónica por lo que existe un vacío jurídico al respecto que requiere ser tutelado en forma específica. p.p 100 y 101.

Del razonamiento antes expuesto, es prudente considerar que para el caso de futuras reformas a la Ley Especial contra los delitos informáticos, se incorpore la definición de Firma electrónica en todas sus acepciones, que el objeto de la Ley exprese claramente que protege, (además de los sistemas que utilicen tecnologías de información), la firma electrónica e igualmente se incorpore el delito de Revelación indebida de la firma electrónica.

2.3 La Biometría

En Venezuela, el uso de la biometría no está previsto de manera expresa, sin embargo, la Ley sobre Mensaje de Datos y Firmas Electrónicas, regula la firma electrónica de forma amplia lo cual despliega la posibilidad del uso de firmas basadas en sistemas biométricos para futuros contratos electrónicos. Conforme lo anterior, cabe señalar que en Venezuela, el evento mas conocido en donde se ha aplicado una técnica biométrica de identificación es el de las Capta Huellas Digitales que se ha estado implementando en las votaciones planificadas por el Consejo Nacional Electoral (CNE), igualmente en el Servicio Administrado de Identificación Migración y Extranjería (SAIME), se utiliza el sistema biométrico de la firma y

el capta huellas digital, al igual que algunas empresas o instituciones la utilizan para el control de asistencia del personal.

No obstante lo anterior, en la actualidad el Banco Provincial implementó la Zona Express, que son cajeros especializados integrados en las oficinas comerciales del país, cuenta con múltiples funciones y además de efectuar las transacciones tradicionales, se pueden realizar: depósitos, actualizaciones de libretas de ahorro y el sistema de cobro de pensión a través de la huella dactilar, esta entidad financiera es la primera en el país que ofrece el uso de la biometría para una transacción bancaria.

Las técnicas de autenticación biométrica más extendidas y aplicables son: el reconocimiento de huella dactilar, el reconocimiento facial, el reconocimiento de voz, el reconocimiento de la forma de la mano, el reconocimiento del iris y el reconocimiento de la firma. Frente a cualquier técnica seleccionada para una determinada aplicación, existe la necesidad de ponderar sus restricciones o peculiaridades, entre ellos se encuentran:

- La necesidad de un dispositivo de adquisición específico en el que esté el usuario.
- Posible variación del patrón a identificar.
- Probabilidad de error individual de cada una de las técnicas.
- Aceptación por parte del usuario de cada una de las técnicas, es decir, si son cómodas, si protegen la privacidad, si son sencillas, etc.

La principal ventaja de este medio de identificación de los sujetos que participan en una operación de comercio electrónico es que los rasgos fisiológicos son únicos y no pueden ser sustraídos a diferencia de lo que ocurre con las claves empleadas en el sistema de criptografía, además es necesaria la presencia física del individuo frente al sistema biometrico, sin embargo, Torres (2005) sostiene:

La biometría presenta un inconveniente que por el momento obstaculiza su desarrollo como medio de seguridad jurídica en el comercio electrónico. Este inconveniente es el elevado costo de la implementación de la tecnología necesaria, pues se requiere de una infraestructura mucho más avanzada que la necesaria para el empleo de la criptografía. p. 211.

Aunado a lo anterior, otro inconveniente es que las características fisiológicas de los seres humanos pueden cambiar con el tiempo, no obstante, esto puede ser superable, indudablemente el costo que implica proteger los sistemas de comunicación es considerable, pero realmente necesario, ya que los avances tecnológicos implican avances en la infraestructura de los sistemas de seguridad, para evitar ser víctima de delitos informáticos y de igual manera controlar la competitividad y los ingresos en una empresa.

Luego de analizados algunos de los sistemas de seguridad en Internet, es menester significar que, para que cualquier intercambio de información o transacción comercial a través de Internet pueda considerarse segura, debe garantizar los siguientes aspectos:

- **Confidencialidad.** Es decir, que debe garantizarse que la información enviada sólo puede ser leída por personas debidamente autorizadas.
- **Integridad.** Debe garantizarse que la información no pueda ser alterada en el transcurso hacia su destino.
- **Autenticación.** Debe garantizarse que los participantes en el intercambio de información o transacción son realmente quienes dicen ser.
- **No Repudio.** Debe garantizarse que ninguna de las personas involucradas en la transacción, puedan negar, posteriormente el hecho de haber participado en la misma.

En este mismo orden de ideas, se sostiene que para que puedan cumplirse todos estos requisitos, es necesario implementar mecanismos de encriptación de la información y firmas electrónicas con sus respectivos certificados electrónicos.

Es importante tener en cuenta, que este medio de seguridad garantiza la eficacia jurídica de los actos que se realizan en Internet, además que está íntimamente relacionados con los avances tecnológicos, es decir, evolucionarán en la medida de que evolucione la tecnología y cualquier nueva invención tecnológica que tenga como objeto proporcionar seguridad en las transacciones comerciales tecnológicas deberá ser considerada un medio de seguridad jurídica, esta idea tiene su fundamento en la aplicación del principio de equivalencia funcional.

Las modalidades y variedades de sistemas de seguridad son innumerables. Sin embargo, en este trabajo hemos mencionado los medios principales, más comunes y más seguros diseñados hasta el momento.

3. Desarrollar de manera crítica los tipos penales aplicables a la contratación electrónica.

En este punto, se desarrollarán la estructura básica y complementaria de los tipos penales aplicado en los contratos electrónicos, de igual manera se afirma que estos tipos pueden cambiar de acuerdo a el avance tecnológico y modos de comisión de delito.

Delito de oferta engañosa.

Para que una empresa logre tener posicionamiento en la web y obtenga útiles ganancias, se requiere de publicidad como medio principal

para ofrecer bienes y servicios a potenciales clientes, sin embargo, es importante que los productos o servicios muestren sus verdaderas cualidades y su calidad real, pues de lo contrario, creará desconfianza en los clientes, afecta su patrimonio, perjudica a los competidores e inclusive podría enmarcarse su conducta en el delito de Oferta Engañosa, tipificado en el artículo 26 de la Ley Especial contra los Delitos Informáticos, el cual es del tenor siguiente:

Artículo 26. Oferta Engañosa. Toda Persona que ofrezca, comercialice o provea de bienes o servicios, mediante el uso de tecnología de información y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta, de modo que pueda resultar algún perjuicio para los consumidores, será sancionada con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave.

A continuación se presentará el desglose de la estructura típica de este delito, en atención al conocimiento penal de esta investigadora, siendo el siguiente:

Artículo 26 de la Ley Especial contra Los Delitos Informáticos.

Sujeto Activo: Indeterminado

Sujeto Pasivo: Determinado (Consumidores)

Objeto Material: Tangible (bienes) e Intangibles (Servicios)

Objeto Jurídico: El Orden Económico

Verbo Rector, es complejo alternativo: Alegar o Atribuir

Penalización: pena a imponer: de uno a cinco años de prisión y multa de 100 a 500 Unidades Tributarias.

Circunstancias de Modo: Ofrecer, comercializar, proveer

Medio de comisión: utilizando tecnología de Información

Instrumentos: computadora

Es un delito de acción pública, simple o mera actividad que castiga la acción, no es un delito de resultado, basta con realizar la conducta típica. Afecta directamente el orden económico, consistente en la intervención del Poder Público para la organización y desenvolvimiento de la economía de un país, referido a la regulación jurídica en la producción, distribución y consumo de bienes y servicios, es un delito que no admite tentativa ni frustración y protege más a consumidores que a competidores.

Es importante señalar que, la oferta engañosa es considerada delito únicamente para el comercio electrónico, pues para el comercio tradicional, es sancionable por vía administrativa, con fundamento en la Ley para la Defensa de las Personas en el Acceso a los Bienes y Servicios, artículo 57 en armonía con el artículo 130 ejusdem, siendo el Instituto para la Defensa de las Personas en el Acceso de Bienes y Servicios (INDEPABIS), adscrito al Ministerio del Poder Popular para el Comercio, el organismo encargado de regular este ilícito administrativo.

Igualmente cuando en la oferta engañosa, el afectado no es el consumidor sino el competidor, las sanciones aplicadas por disposición de la Ley para promover y proteger el ejercicio de la libre competencia, artículo 17 numeral 1 en armonía con el artículo 49, son igualmente administrativas y el organismo encargado para regular este ilícito administrativo es la Superintendencia para la promoción y protección de la libre competencia, adscrita al referido Ministerio.

Delito de estafa

Seguidamente, se describe uno de los delitos más comunes en toda la humanidad, teniendo en cuenta que de todas las defraudaciones informáticas que existen, la más frecuente es la del delito de estafa, tipificado en el artículo 462 del Código Penal Venezolano, el cual es del tenor siguiente:

El que, con artificios o medios capaces de engañar o sorprender la buena fe de otro, induciéndole en error, procure para sí o para otro un provecho injusto con perjuicio ajeno será penado con prisión de uno a cinco años. La pena será de dos a seis años si el delito se ha cometido:

1. En detrimento de una administración pública, de una entidad autónoma en que tenga interés el Estado o de un instituto de asistencia social.

2. Infundiendo en la persona ofendida el temor de un peligro imaginario o el erróneo convencimiento de que debe ejecutar una orden de la autoridad.

El que cometiere el delito previsto en este artículo, utilizando como medio de engaño un documento público falsificado o alterado, o emitiendo un cheque sin provisión de fondos, incurrirá en la pena correspondiente aumentada de un sexto a una tercera parte.

Estructura típica de este delito, artículo 462 del Código Penal Venezolano.

Sujeto Activo: Indeterminado

Sujeto Pasivo: Plurisujetividad Pasiva, es decir, Indeterminado en el encabezamiento del artículo y Determinado en el Primer Aparte (El Estado).

Objeto Material: Intangible y Tangible

Objeto Jurídico: La Propiedad

Verbo Rector, es simple: Procurar (un provecho en perjuicio ajeno)

Penalización: pena a imponer: Tres (03) años de prisión para el encabezamiento y cuatro (04) años para los siguientes supuestos, tiene una agravante de 1/6 a 1/3 parte de la pena correspondiente.

Circunstancias de Modo: Engañando o sorprendiendo la buena fe y en el segundo numeral infundiendo el temor de un peligro o en error para ejecutar una orden de la autoridad

Medios de comisión: Con artificios o medios y en el último aparte, con documento publico falsificado o alterado o con cheque sin provisión de fondos.

Es un delito de acción publica, que puede ser cometido por personas naturales o jurídicas, admite el grado de tentativa y frustración, sin embargo es un delito de resultado, puesto que exige para su consumación el daño patrimonial ajeno, además requiere que el presupuesto subjetivo del dolo sea plenamente demostrado, es decir, que determine visiblemente el ánimo de engañar y el presupuesto objetivo de la conducta es procurarse un provecho injusto en perjuicio ajeno, ese dolo debe ser preciso e incuestionable y debe ser anterior a la prestación patrimonial, la estafa ha sido diseñada con un componente intelectual original (engaño, sorprendiendo la buena fe), es por ello que la relación jurídica inicial es considerada ilegítima y en consecuencia nula por existir vicio en el consentimiento de la victima.

El error, refleja una representación equivocada de la realidad y constituye el nexo entre el engaño y el perjuicio patrimonial, sin embargo es importante destacar que el error es un elemento separado del engaño pero valorar el error aisladamente no constituye el tipo de estafa, puesto que el resultado de este tipo penal es el perjuicio patrimonial.

Entre las estafas más comunes que pueden llevarse a cabo por Internet, están: La oferta de bienes y servicios, oportunidades de negocios que con una pequeña inversión económica ofrece grandes beneficios, en ambos casos luego de haberse hecho la transacción monetaria, el sitio web que ofrecía la oferta no responde con las condiciones pactadas o no existe; igualmente la solicitud por e-mail de datos personales y contraseñas bancarias, que además nos lleva a un enlace que aparenta una real pagina web de banco, institución, empresa u organismo que se pretenda suplantar (conocido como phishig); las ofertas falsas de trabajo, la suscripción de servicios gratuitos, pero que no lo son y condicionan el envío del numero de tarjeta de crédito como garantía o algún otro artificio capaz de engañar al usuario.

Actualmente existe una nueva forma de Estafa bajo la modalidad de Phishing, distinta a aquella que nos lleva a un enlace en la web para capturar los datos de las personas, contraseñas y números de tarjetas de crédito y el jurista Zapata (2009), lo explica así:

Un procedimiento más sofisticado es la instalación de un programa espía en la computadora personal. A través de un programa espía, se vigila la actividad del usuario, por ejemplo la contraseña tecleada cuando se conecta con su banco. Se instala en la computadora a través de un anexo a un correo electrónico, o escondido en un archivo de fotos o de música descargada gratuitamente de la web. Este programa espía, gusano electrónico programa troyano, puede ser capaz de mutarse para evitar la detección de un programa antivirus, y pasar desapercibido durante mucho tiempo. Envía la información deseada a un destino oculto, y se autodestruye para que el usuario no se de cuenta de que su información confidencial ha sido espíada. Posteriormente, la información obtenida se puede utilizar para vaciar cuentas bancarias o acceder a servidores protegidos con contraseña.

p. 34

Como se aprecia, existen innumerables maneras de cometer defraudaciones en Internet y cada día existirán mejores técnicas de cometer este tipo de delito, por ello es importantísimo para una empresa o persona

natural ser muy cuidadoso cuando se suministre información personal o financiera a través de Internet y nunca responder solicitudes de información personal a través de correos electrónicos.

No obstante lo anterior, existen recomendaciones para evitar que nuestro patrimonio sea objeto de este delito, en el caso de solicitar un bien o servicio por Internet, es necesario ingresar a paginas que estén plenamente identificadas, con su dirección real y teléfono de contacto, igualmente hay que verificar que el sitio tenga un dominio de pago y no un subdominio en un hosting gratuito, pues muchas veces los estafadores compran un dominio y utilizan el subdominio gratuito para cometer este delito, de tal manera que no sea cerrado por el dueño del host (que es la compañía que ofrece servicio de alojamiento para paginas web).

Para el caso de compras por Internet o transacciones en las paginas web de agencias tributarias, bancos u otras instituciones financieras, es importante teclear la dirección directamente en el navegador y no ingresar a través de enlaces, compruebe que antes de ingresar su clave, en esa pagina haya una "S" luego de las letras "http", por ejemplo: en la pagina del Banco de Venezuela, al ingresar al link personal Express aparecerá: (<https://e-bdvcpx.banvenez.com/registroclavenetpersonal>), esa letra "s" luego del http, significa seguro, también para comprobar la certificación de autenticidad de la pagina debe aparecer en la parte inferior o superior derecha un candado dorado o una llave.

Delito de fraude electrónico.

Continuamos con el delito de fraude electrónico, previsto y sancionado en el artículo 223 de la Ley de las Instituciones del Sector Bancario, el cual reza así:

“Quien a través de la manipulación informática o mecanismo similar, con ánimo de lucro, efectúe una transferencia o encomienda electrónica de bienes no consentida, en perjuicio de la institución del sector bancario o de un usuario o usuaria, será penado con prisión de ocho a diez años.

Con la misma pena serán castigados las personas naturales identificadas en el artículo 186 de la presente Ley o los empleados de la institución del sector bancario, que colaboren en la comisión de las transferencias antes mencionadas.”

Siendo su estructura típica:

Artículo 223 de la Ley de las Instituciones del Sector Bancario.

Sujeto Activo: Es Plurisujetivo, Indeterminado y Determinado en el Primer aparte (sujetos que establece el artículo 186 ejusdem).

Sujeto Pasivo: Determinado (Usuario e Institución del Sector Bancario).

Objeto Material: Tangible (lucro-bienes)

Objeto Jurídico: Es Pluriofensivo: La Propiedad y el Orden Económico

Verbo Rector: Es complejo alternativo: Efectuar o Colaborar

Penalización: pena a imponer: de ocho a diez años de prisión.

Circunstancia de Modo: Transferencia o encomienda electrónica de bienes no consentida

Medio de comisión: manipulación informática o mecanismo similar

Instrumentos: Tecnologías de Información

Del mismo modo que la Estafa, es un delito doloso y ese dolo recae sobre la conducta de efectuar o colaborar en realizar una transferencia electrónica de bienes no consentida, al no haber consentimiento quien

provee el bien incurre en error y quien obtiene el bien en dolo, lo cual hace que la relación jurídica previa sea ilegítima, existe plurisujetividad activa, puesto que en el primer aparte realiza una remisión contextual dirigida a todo el personal que rige las instituciones bancarias incluyendo los de la Superintendencia de Bancos, es un delito que admite la frustración y se incluye en esta investigación, porque todas las transacciones bancarias son consideradas contratos electrónicos.

En mi opinión, el principal afectado en este delito es la Institución Financiera, pues según la Superintendencia de Bancos (SUDEBAN), estas deben responder con prontitud todas las denuncias de usuarios cuyas cuentas han sido violentadas, hoy día es el delito más común en el sistema financiero, a tal punto que las empresas aseguradoras no cubren los costos que implica el fraude electrónico al que esta sometido todo el sistema público y privado, siendo una de las principales preocupaciones que ha impulsado a la banca a tomar medidas urgentes para blindarse contra este delito.

Un de esas medidas es la sustitución de tarjetas de crédito y debito de banda magnética por las de tecnología chip, otra es que han implementado la biometría en los cajeros, igualmente las campañas publicitarias de prevención de reconocimientos de correos fraudulentos, la implementación de las tarjetas de coordenadas para las transacciones bancarias, entre otros, sin embargo, la velocidad del cambio dependerá de la capacidad de inversión de cada banco.

Al respecto la autora, Granadillo (2009), señala:

“Por otra parte, la descripción prevista en este tipo penal, supone que la acción debe desplegarse en perjuicio del banco, entidad de ahorro y préstamo, institución financiera o casa de cambio, o de un cliente o usuario.

Sin embargo, respecto al delito cometido en perjuicio de un cliente o usuario, es relevante acotar que la Ley contra los Delitos Informáticos, tipifica en su artículo 14 el delito de “fraude”, dentro del grupo de los delitos contra la propiedad, figura en la cual es subsumible en forma genérica, cualquier conducta fraudulenta cometida a través de medios informáticos de las cuales se obtuviera un provecho injusto en perjuicio ajeno.” p. 35

Ciertamente, el artículo 14 de la Ley Especial contra los delitos informáticos, tipifica el delito de fraude de una manera muy genérica y en la práctica reiteradamente este delito se encuadra en la conducta de extraer dinero de los cajeros automáticos, por esta razón se optó como objeto de estudio el tipo de Fraude Electrónico tipificado en la Ley de Instituciones para el sector bancario, ya que se relaciona directamente con las transferencia o encomienda de bienes no consentida, siendo esta acción la más armónica a lo que refiere el objeto de estudio de este trabajo que es la contratación electrónica.

www.bdigital.ula.ve

CAPITULO V.

CONCLUSIONES Y RECOMENDACIONES

Como se ha dicho, los avances tecnológicos y su importancia en el mundo de los negocios, ha hecho considerar para Venezuela impostergable adaptar las normas jurídicas a dichas eventualidades. Se pudo observar que la contratación electrónica es perfectamente válida, puesto que, el valor probatorio del documento electrónico está plenamente admitido en Venezuela, en el artículo 4 de la Ley sobre Mensajes de Datos y Firmas Electrónicas (LSMDFE), con un criterio específico para la promoción, control, contradicción y evacuación de la prueba, que se realizará como medios de prueba libre, tal como lo prevé el Código de Procedimiento Civil.

Sin embargo, en virtud del principio de equivalencia funcional, se creó la convicción de que los Documentos Electrónicos avalados con Firmas Electrónicas que utilicen un certificado emitido por un Proveedor de Servicios de Certificación Electrónica acreditado por la Superintendencia de Servicios de Certificación Electrónica (SUSCERTE), tendrán la misma eficacia y validez del documento escrito y la firma manuscrita respectivamente, en consecuencia pueden ser valoradas como pruebas documentales propiamente dichas y no como un medio de prueba libre.

Igualmente, para que la Firma electrónica tenga su plena validez y eficacia probatoria, además de estar debidamente certificada por un Proveedor de Servicios de Certificación Electrónica acreditados por la Superintendencias de Servicios de Certificación Electrónica (SUSCERTE), deberá cumplir con los aspectos establecidos en el artículo 16 de la Ley sobre Mensajes de Datos y Firmas Electrónicas, de lo contrario se constituirá

como un elemento de convicción valorable en juicio conforme a las reglas de la sana crítica.

Con respecto a los elementos para la existencia de los contratos, se pudo apreciar que la forma por excelencia de manifestar el consentimiento es a través de un mensaje de datos, sin embargo, se debe tener especial cuidado con este elemento del contrato y para ello se debe implementar los mecanismos de la firma electrónica. El objeto no representa diferencia alguna en un contrato electrónico y la causa no se ve afectada por el hecho de que éste se celebre por vía electrónica. Además, se pudo apreciar que para identificarse electrónicamente debe hacerse través de la firma electrónica, sin embargo es de carácter supletorio y solo es aplicable en caso que las partes no hayan acordado previamente un procedimiento alterno.

La tecnología ha implementado soluciones para la seguridad en las transacciones por la Internet, como es el caso de La firma electrónica, la cual es altamente segura y para su elaboración, requiere de aplicaciones criptográficas lo cual permite que sus trámites sean confiables. De igual manera, la criptografía cuyo principio básico es mantener la privacidad de la comunicación, entre personas, alterando el mensaje original, y la biometría que ofrece la mejor de las garantías con respecto a la identificación de personas y su función en el comercio electrónico es garantizar la identidad de los sujetos que participan en él.

Aunado a lo anterior, existe la necesidad de implementar Legislaciones que atiendan el problema jurídico de la inseguridad en las transacciones electrónicas y comercio electrónico en general, en Venezuela existe la Ley Especial contra los delitos informáticos moderadamente acorde con las nuevas tecnologías, pues si bien atiende a la protección de los bienes jurídicos como; la propiedad, la privacidad de las personas y las

comunicaciones y el orden económico, no ha implementado en su articulado disposiciones que regulen a la Firma electrónica (la cual soluciona uno de los problemas legales más grandes del comercio electrónico como es la inseguridad), convirtiéndose en una necesidad impostergable, puesto que, la legislación le otorga su reconocimiento jurídico, validez y eficacia probatoria, mas no existe regulación completa desde el punto de vista delictivo.

En lo que respecta al delito de Oferta engañosa, considerarlo delito únicamente para el comercio electrónico, tiene su razón de ser, en el sentido de que la oferta electrónica es una proposición unilateral que una de las partes dirige a la otra para celebrar un contrato y no es considerado un acto preparatorio sino una declaración contractual que entiende, que el contrato ha sido cerrado con la sola aceptación de la otra parte, por tal motivo el legislador exige que la oferta deba ser completa con todos los requisitos esenciales de un contrato.

Finalmente se destaca que el delito de Estafa es uno de los más comunes en las defraudaciones informáticas, que requiere de un elemento intelectual original como lo es el engaño y para su consumación es necesario el perjuicio patrimonial; para el caso del fraude electrónico, es un delito que perjudica más a la Instituciones Bancarias que a los consumidores y actualmente es el delito más común en todo el sistema financiero.

Recomendaciones

Ante el advenimiento de nuevos desarrollos tecnológicos y aún cuando la Ley Sobre Mensajes de Datos y Firmas Electrónicas se basó en los principios de equivalencia funcional, neutralidad tecnológica y autonomía de voluntad con el fin de la no modificación del derecho, se recomienda la reconsideración en el ordenamiento jurídico vigente sobre los conceptos tradicionales en materia de derechos de contratos, puesto que en sus

definiciones se evidencia que el elemento informático es un medio esencial para la contratación.

Igualmente se recomienda, que para futuras reformas de la Ley Especial contra los delitos informáticos, se regulen los mecanismos de encriptación o protocolos de seguridad en las transacciones en aras de resguardar la seguridad, integridad, autenticación y no repudio de las partes contratantes, que es el tema de valor de las llamadas firmas electrónicas.

Para evitar estafas o cualquier defraudación informática, se exhorta a mantenerse informado de las nuevas modalidades de comisión de estos delitos, ser muy cuidadoso cuando se suministre información personal o financiera a través de la Internet, no responder información personal de correos electrónicos ni acceder a paginas de bancos a través de enlaces, sino teclear el dominio directamente en el navegador, verificar que el servidor este protegido con los protocolos de seguridad ([HTTPS://](https://)) y aparezca el candado dorado en la parte superior cerrado.

Para las sociedades mercantiles, es importante que inviertan en tecnología, igualmente notificar inmediatamente a la entidad financiera, si sospecha que ha sido victima de un delito de estafa, robo de claves de acceso o tarjetas inteligentes, verificar constantemente sus estados de cuenta y evitar hacerlo en sitios públicos. Hay que actuar en forma inmediata si se sospecha de alguna irregularidad relacionada con delitos en las contrataciones, puesto que la evidencia puede ser borrada o modificada por las personas que tienen a cargo el control de la información.

REFERENCIAS

Acedo Mendoza Manuel y Acedo de Lepervanche Luisa (1991). **La Sociedad Anónima**. Caracas: Vadell hermanos

Angel Angel José de Jesús. **Criptografía para principiantes**. [Documento en línea], Disponible en: www.hacienda.go.cr/centro/datos/.../Criptografia%20Básica-Principiantes.pdf [Fecha de consulta: 19-October-2012].

Arango Rueda Adriana. (Comp.). (2002). **Internet, Comercio Electrónico & Telecomunicaciones**. Universidad de Los Andes. Bogotá: Legis

Arias Ferrer María Inés. (2008). **Ley Sobre Mensajes de Datos y Firmas Electrónicas, comentarios a la Sentencia de fecha 12 de febrero de 2008**. Fronesis Revista de Filosofía Jurídica, Social y Política. [Revista en Línea]. Disponible en: <http://revistas.luz.edu.ve/index.php/frone/article/viewfile/1853/1794>. [Fecha de Consulta: 24-Abril-2010]

Barboza P. Ely S. (2007). **Derecho Mercantil**. Bogotá: McGraw - Hill

Constitución de la República Bolivariana de Venezuela. Gaceta Oficial de la Republica Bolivariana de Venezuela N° 36.860 del 30 de diciembre de 1.999

Código Civil de Venezuela. Gaceta Oficial de la Republica de Venezuela N° 2.990 del 26 de julio de 1.982.

Código de Comercio. Gaceta Oficial de la Republica de Venezuela N° 475 Extraordinario del 21 de diciembre de 1.955.

Código Penal Venezolano. Gaceta Oficial de la República Bolivariana de Venezuela N° 39.818 de fecha: 12 de Diciembre de 2011.

Del Carpio Narváez Luis A. (2009). **La Contratación Electrónica.** [Documento en línea], Disponible en: <http://www.derechoycambiosocial.com/> [Fecha de la consulta: 24-Abril-2010]

Devis Echandía Hernando. (1993). **Teoría General de la Prueba Judicial.** Medellín: Biblioteca Jurídica Diké.

Díaz Solange (2008). **Lineamientos para una Propuesta de Normativa Jurídica que Regule a las Sociedades Mercantiles, como Sujetos Activos de Delito en el Comercio Electronico, a partir del Análisis Comparativo con el Derecho Español.** Trabajo Especial de Grado no publicado. Universidad de los Andes, Mérida Venezuela

Ditotto Beatriz (2010). **Los tipos penales en la Ley Especial contra los Delitos Informáticos.** [Documento en línea]. Disponible en: <http://beatrizditotto.net/2010/01/>. [Fecha de consulta: 04-Diciembre-2011]

Domingo Gonzalo Ernesto. (2004) **Seguridad en las transacciones On-Line de Comercio Electronico.** [Documento en línea]. Disponible en: <http://campus.dokeos.com/courses/0025/document/certificates/comercio.pdf> [Fecha de consulta: 12-Enero-2011]

España Boquera María Carmen (2003) **Servicios Avanzados de Telecomunicación**. [Documento en línea.] Disponible en: <http://books.google.co.ve/books> [Fecha de consulta: 13-Abril-2011]

Gabaldon Luis Gerardo y Nicanora Becerra (2008). **Variables agotadas a la consumación y al agotamiento del fraude mediante transferencias bancarias por vía electrónica**. [Documento en línea]. Disponible en: www2.scielo.org.ve/scielo.php?script=sci_arttext&pid. [Fecha de consulta: 20-Mayo-2010].

Granadillo Colmenares, Nancy C. (2008). **Los Delitos Bancarios**. Caracas: Vadell Hermanos.

González H. Horacio Jesús. (2009). **Valor Probatorio del Documento Electrónico**. Revista de Derecho Probatorio N° 15. Caracas: Ediciones Homero.

Haig, Matt. (2001). **Fundamento del Comercio Electrónico**. Barcelona: Gedisa.

Landáez Otazo, Leoncio A. (2009). **El Comercio Electrónico, nueva tecnología e Internet**. Caracas: Vadell Hermanos.

Landáez Otazo, Leoncio A. (2009). **Perfeccionamiento del Contrato Electrónico**. [Documento en línea]. Disponible en: <http://www.entorno-empresarial.com/> [Fecha de consulta: 24-Abril-2010]

Lerma Hector (2004). **Metodología de la Investigación**. Segunda Edición. Bogotá: Ecoe Ediciones

Ley de Mensaje de Datos y Firmas Electrónicas. Gaceta Oficial de la Republica Bolivariana de Venezuela N° 37.148 del 28 de febrero de 2001.

Ley de Instituciones del Sector Bancario. Gaceta Oficial de la República Bolivariana de Venezuela N° 39.627 del 02 de Marzo de 2011

Ley sobre los delitos Informáticos. Gaceta Oficial de la Republica Bolivariana de Venezuela N° 37.313 del 30 de octubre de 2001.

Ley para la Defensa de las Personas en el Acceso a los Bienes y Servicios. Gaceta Oficial de la República Bolivariana de Venezuela N° 39.358 del 01 de febrero de 2010.

Lozada Yenicce Dayana (2010). **Importancia y Validez de los Contratos Electrónicos en el Ordenamiento Jurídico Venezolano y su relación con el Comercio Electrónico.** Trabajo Especial de Grado no Publicado. Universidad de Los Andes. Mérida Venezuela.

Maduro L. Eloy y Pittier S. Emilio. (2002). **Curso de Obligaciones, Derecho Civil III.** Caracas: Publicaciones UCAB.

Moreno Luciano. (2002). **Criptografía.** [Documento en línea]. Disponible en: http://www.terra.es/personal6/morenocerro2/seguridad/cripto/cripto_13.html [Fecha de consulta: 14-Octubre-2012].

Perez Bonachea Mayren (2010). **Problemática de los vicios del consentimiento en la contratación celebrada mediante las nuevas tecnologías de la información.** [Revista en línea N° 147]. Disponible en: <http://www.alfa-redi.org/node/8817>. [Fecha de consulta: 14-10-2012]

Pérez Sarmiento Eric. (2005). **La Prueba en el Proceso Penal Acusatorio**. Caracas: Vadell hermanos.

Reyes Alvarado Yesid. (1996). **Imputación Objetiva**. Bogotá: Temis S.A

Rico Carrillo, Mariliana. (2005). **El Comercio Electrónico Internet y Derecho**. Segunda Edición. Bogotá: Legis.

Rincón Cardenas, Erick. (2006). **La Contratación Electrónica**. Bogotá: Universidad del Rosario.

Ruiz Wilmer de Jesús. (2010). **Criminalística, nuevos métodos y técnicas**. Primera Edición. Lara: Horizonte C.A.

Salgueiro Araujo, José (2001). **Contratación Electrónica**. [Documento en línea]. Disponible en: <http://www.alfa-redi.org> [Fecha de consulta: 24-Abril-2009]

Soto Coaguila Carlos A. (2001). **El Comercio Electrónico en el Derecho Peruano**. [Documento en línea]. Disponible en: <http://www.alfa-redi.org> [Fecha de consulta: 24-Abril-2009]

Superintendencia de Servicios de Certificación Electrónica. Portal Web. www.suscerte.gob.ve

Tamayo Mario. (2004). **El Proceso de la Investigación Científica**. Mexico: Editorial Limusa S.A de C.V

Torres A. Hernán (2005). **Sistema de Seguridad Jurídica en el Comercio Electrónico**. Lima: Fondo Editorial de la Pontificia Universidad Católica del Perú

Tribunal Supremo de Justicia. Portal Web. www.tsj.gob.ve

Universidad de los Andes. (Comp.). (2005). **Derecho de Internet & Telecomunicaciones**. Bogotá: Legis.

Universidad Pedagógica Experimental Libertador. (2006). **Manual de Trabajos de Grado de Especialización y Maestrías y Tesis Doctorales**. Caracas: Fedupel.

Velasquez Velasquez Fernando. (2002). **Manual de Derecho Penal. Parte General**. Bogotá: Temis

Zapata Marcó Juan Carlos (2009) **La Estafa en la modalidad de “Phishing” a través de Internet y sus Medios Probatorios en Venezuela**. Trabajo Especial de Grado. [Documento en línea], Disponible en: <http://riuc.bc.uc.edu.ve/bitstream/123456789/148/1/11009.pdf> [Fecha de consulta: 18-Octubre-2012].