REPUBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JOSE ANTONIO PAEZ

FACULTAD DE CIENCIAS JURIDICAS Y POLITICAS

ESCUELA DE DERECHO

IMPORTACIA DE LOS DELITOS INFORMÁTICOS PREVISTO EN LA LEY ESPECIAL

Autor(a) Villarreal G Margareth C.

C.I: V-24.644.303

Tutor académico: Dr. Germán brea**.**

San diego, enero 2019

REPUBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JOSE ANTONIO PAEZ

FACULTAD DE CIENCIAS JURIDICAS Y POLITICAS

ESCUELA DE DERECHO

IMPORTACIA DE LOS DELITOS INFORMÁTICOS PREVISTO EN LA LEY ESPECIAL

CONSTANCIA DE ACEPTACION

Nombre, Apellido, Cedula de identidad y Firma del Tutor Académico

---

Nombre, Apellido, Cedula de Identidad. Firma jurado I

Nombre, Apellido, Cedula de Identidad. Firma Jurado II

San Diego, Enero 2019.

RECONOCIMIENTOS

A dios primeramente por darme la oportunidad de vivir, guiarme en el camino y darme la fuerza necesaria para superar todos los obstáculos y alcanzar el éxito.

A la universidad José Antonio Páez por abrirme las puertas y permitirme realizar mis estudios, gracias por aportarme conocimientos por brindarme la oportunidad de crecer como persona desde el primer día de clase en la facultad de ciencias jurídicas y políticas por forjar mi carácter en la escuela de derecho y darme las herramientas para llegar hacer una gran abogada.

A mi madre Edilia Gamarra y mi padre Otilio Villarreal, por creer en mí por su confianza por su entrega total y su apoyo en mi vida por impulsarme en los momentos más difíciles y por el orgullo que siente hoy en día por mí.

A mis profesores German brea, libia villa, Olga matos por impartirme y regalarme parte de sus conocimientos por demostrar interés y colaborarme con la construcción de un trabajo de grado de buen nivel. Y que alguna u otra manera fomentaron en mí el deseo de superación y que marcaron cada etapa de mi camino universitario.

A mis compañeros quienes desde el primer día clases en esta carrera me dieron su apoyo y ayudaron durante todo el periodo de estudio en la universidad.

AGRADECIMIENTOS

Dedico este trabajo y toda mi carrera universitaria a dios, por estar siempre a mi lado y guiándome en todo momento, dándome amor, fuerzas y bondad para seguir creciendo como persona afrontado todos los obstáculos que se me presenten día tras día.

Gracias a mis padres Edilia gamarra y Otilio Villarreal por haberme forjado como la persona que soy en la actualidad; porque lucharon por mi bienestar, por mi educación y mi salud. No conozco a nadie en este mundo a quienes les deba más amor y agradecimiento, todos mis logros se los debo a ustedes. Le doy muchas gracias a dios por lo bendecida que soy de tenerlos como padres mil gracias.

A mis hermanos Jhon Erick, Cristian Enrique y Richard Antonio por estar siempre a mi lado, por apoyarme, por guiarme también hacia un buen camino y apoyarme frente a las adversidades de la vida y apoyándome para seguir adelante en mis estudios.

Mi tío Gilberto forero que también forma parte de este gran logro en mi vida, por sus consejos y apoyo constitucional.

A mis abuelos maternos Margarita plata y Alfredo gamarra y paternos Gilma María el Jach y Cesar Augusto Villarreal. Que desde el cielo me guían mis pasos cada día, me ayudan a perseguir los sueños que un día decidí que quería alcanzar y que sin duda como mis ángeles me han ayudado a convertirme en la persona que soy ahora.

A mi tía Anita gamarra que sin duda alguna estuvo apoyándome en todo momento, sé que no tuve la oportunidad de compartir en persona este logro, pero sé que desde el cielo estás orgullosa de mi. Gracias tía por estar conmigo, por guiarme en mis metas por haber compartido cosas inolvidables contigo siempre te tendré presente como otro ángel más en vida.

INDICE

REPUBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JOSE ANTONIO PAEZ

FACULTAD DE CIENCIAS JURIDICAS Y POLITICAS

ESCUELA DE DERECHO

IMPORTACIA DE LOS DELITOS INFORMÁTICOS PREVISTO EN LA LEY ESPECIAL

Autor: Margareth Villarreal

Tutor Académico: Germán brea.

RESUMEN

Debido a que en la actualidad existen muchas maneras para hacer fraude, se tiene la necesidad de dar a conocer los distintos tipos de delitos informáticos, así como su finalidad la que llegan las personas responsables de estos ilícitos.

En la actualidad la sociedad se desenvuelve cada vez más entre la tecnología, por lo que provoca que se depender de la misma. Compras y ventas por internet, transacciones electrónicas ya sean bancarias o de efectivo, comunicación por internet, entre otras. Y más las razones por las que la sociedad se involucra altamente en la tecnología y por tanto toma cierto peligro al ser defraudados por delincuentes de la informática.

Los delincuentes de la informática son tantos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado. Estos delincuentes suelen pasar desapercibidos y sabotean las computadoras para ganarles ventaja económica.

Descriptores: Delitos informáticos, sabotaje, informática, ciberterrorismo, antijurídico.

INTRODUCCIÓN

En este proyecto se analizará el impacto que tienen los delitos informáticos, ya que son muchas las personas que se comunican, hacen sus compras, pagan sus cuentas, realizan negocios y hasta consultan con sus médicos por medio de redes computacionales. Los delincuentes de la informática son tantos como sus delitos; puede tratarse de estudiantes, terroristas o figuras del crimen organizado.

Los efectos de la revolución digital se hacen sentir en los distintos sectores de la sociedad como lo es en la economía, la política, la educación, el entretenimiento entre otras. Así pues, la sociedad en el ámbito digital encontró unas nuevas formas de interrelacionarse y este fenómeno ha generado cambios profundos que se irán asentando y evolucionando con el tiempo, por lo que es imprescindible estar preparados para enfrentar una evolución tecnológica acelerada.

Estos delincuentes suelen pasar desapercibidos y sabotean las bases de datos para ganarles ventaja económica a sus competidores o amenazar con daños a los sistemas con el fin de cometer extorsión o manipulan los datos o las operaciones, ya sea directamente o mediante los llamados «gusanos» o «virus», que pueden paralizar completamente los sistemas o borrar todos los datos del disco duro; también han utilizado el correo electrónico y los «Chat rooms» o salas de tertulia de la Internet para buscar presas vulnerables. Por ejemplo, los aficionados a la pedofilia se han ganado la confianza de niños online y luego concertado citas reales con ellos para explotarlos o secuestrarlos.

También se observa que las empresas que poseen activos informáticos importantes, son cada vez más celosas y exigentes en la contratación de personal para trabajar en éstas áreas, pudiendo afectar en forma positiva o negativa a la sociedad laboral de nuestros tiempos. Aquellas personas que no poseen los conocimientos informáticos

básicos, son más vulnerables a ser víctimas de un delito, a diferencia de aquellos que si los poseen.

En vista de lo anterior, aquellas personas que no conocen nada de informática (por lo general personas de escasos recursos económicos) pueden ser engañadas si en un momento dado poseen acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de tecnologías como la Internet y/o correo electrónico.

En la sociedad han sido muchas las víctimas de tales delitos, que han quedado impunes debido a la falta de tipificación, y es que la forma de cometerse no ha sido estudiada, trayendo como consecuencia que exista un vacío legal en la legislación nacional e internacional.

Es por ello que en el tema pues se encuentra de vital importancia la investigación más profunda de estas nuevas formas antijurídicas y por lo tanto, la presente ponencia tiene como objeto fundamental explicar de una manera breve y concisa que son los delitos Informáticos, su caracterización, los sujetos que los realizan, la clasificación de las distintas formas en que se realizan, la legislación comparada que existe en esta materia, un breve sumario de la legislación que existe en la República Bolivariana de Venezuela que regula esta nueva forma de delinquir, y por último, su influencia en la propiedad intelectual. Todo esto a fin de que se tengan una idea general de lo complejo que es la revolución digital y que nuestros gobernantes se adecuen a esta realidad legislando sobre esta materia coherentemente.

Este proceso se describe, en este trabajo, por medio de IV capítulos, distribuidos de la siguiente manera:

En el capítulo I, se plantea y formula el problema que da origen a la investigación, desarrollando los objetivos y metodología a cumplir para su solución; así mismo se presenta la importancia del estudio.

En el capítulo II, se indica la reseña histórica sobre los delitos informáticos en el cual muestra antecedentes y bases teóricas que sustentan la investigación; además de las bases legales bajo los cuales se enmarca la misma.

En el capítulo III, se da a conocer: tipo y métodos de la investigación. También, se describe las fases metodológicas y dejar de manera las fuentes en conocimiento jurídico.

En el capítulo IV se presenta los resultados se exponen las conclusiones y las recomendación sobre este tema por el cual explica la situación actual de los delitos informáticos.

CAPITULO I

EL PROBLEMA

Planteamiento del problema

En la actualidad las computadoras se utilizan no sólo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación fundado en la informática; tecnología cuya esencia se resume en la creación, procesamiento, almacenamiento y transmisión de datos.

La informática está hoy presente en casi todos los campos de la vida moderna con mayor o menor auge. Todas las ramas del saber humano se rinden ante los progresos tecnológicos y comienzan a utilizar los sistemas de información para ejecutar tareas que en otros tiempos se realizaban manualmente.

El progreso de los sistemas informáticos es cada día más importante porque permite procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, que estará al alcance concreto de millones de interesados. Las más diversas esferas del conocimiento humano; en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporadas a sistemas informáticos que, en la práctica cotidiana, entrega con facilidad a quien lo desee, ese conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados.

En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operar, confiables y capaces de responder a casi

toda la gama de interrogantes que se planteen a los archivos informáticos. Puede sostenerse que hoy en dia las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso.

Los doctrinarios consideran que este será el nuevo fenómeno científico-tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse que la informática es hoy una forma de poder social. Las facultades que el fenómeno pone a disposición de gobiernos y de particulares, con rapidez y ahorro consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícitos e ilícitos, en donde es necesario el derecho para regular los múltiples efectos de una situación nueva y de tantas potencialidades en el medio social.

Los progreso de las computadoras a nivel mundial y el creciente aumento de las capacidades de almacenamiento y procesamiento asi como la miniaturización de los microprocesadores de las computadoras instalados en productos industriales, la fusión del proceso de la información con las nuevas tecnologías de comunicación, así como la investigación en el campo de la inteligencia artificial, ejemplifican el desarrollo actual definido a menudo como la "era de la información".

En la actualidad la informatización se ha implantado en casi todos los países, siendo utilizado en la organización y administración de empresas tanto públicas como privadas, teniendo un uso importante en la investigación científica. Su utilización en la producción industrial ha catapultado el desarrollo social, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta, comienzan a surgir algunas facetas negativas y extremadamente dañinas que se conoce como criminalidad informática.

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son

algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales.

Pero no sólo la cuantía de los perjuicios ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que quede impune el delito, ya que se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En consecuencia, la legislación venezolana sobre protección de los delitos informáticos busca cercarse lo más posible a los distintos medios de protección ya existentes, creando en una regulación sólo en aquellos aspectos en los que, en base a las peculiaridades del objeto de protección, sea imprescindible.

Si se tiene en cuenta que los sistemas informáticos pueden proporcionar datos e informaciones sobre miles de personas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades como: bancarias, financieras, tributarias, previsionales y de identificación de las personas, y si a ello se agrega que existen bancos de datos, empresas o entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre materias de las más diversas disciplinas a un Estado o particulares, se comprenderá que están en juego o podrían llegar a estarlo de modo dramático, algunos valores colectivos y los consiguientes bienes jurídicos que el ordenamiento jurídico-institucional debe proteger.

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial. Estas distintas medidas de protección no tienen porque ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas.

La relación con el origen de los delitos informáticos sin duda viene dado por el avance de la tecnología informática en el tiempo y espacio, lo que ha conllevado a

entrelazar la vida real con algún tipo legal, estableciendo así un uso ilícito de las redes mundiales como el internet o correo electrónico; afectando así la privacidad de las personas creando, capturando, grabando, copiando, alterando, duplicando o eliminando la información contenida en los sistemas técnicos informáticos; con el objeto de incorporar usuarios, cuentas, registros o consumos inexistente o la modificación de la cuantía de estos, lo que conlleva al surgimiento de los llamados delitos informáticos.

Es importante resaltar que debido al uso de la tecnología han surgido estas acciones antijurídicas por ello se creó la necesidad de regular este tipo de delitos novedosos que lesiona bienes jurídicos no solo de carácter económico sino también de contenido social, debido a la importancia de velar para que se cumplan los fines establecidos en el ordenamiento jurídico venezolano donde se castigan severamente los delitos cometidos, teniendo así como resultado en la legislación especial venezolana la Ley Especial contra los Delitos Informáticos publicada en Gaceta Oficial el 30 de Octubre del año 2001 con entrada en vigencia en el año 2002, la cual traería consigo seguridad jurídica a los usuarios de los sistemas de información, alertándolos en base a cuando se está frente a un delito informático y cuando no.

En relación a los delitos contra los sistemas que utilizan tecnología están divididos en: el acceso indebido, el sabotaje o daño a sistemas, el favorecimiento culposo de sabotaje o daño, el acceso indebido o sabotaje a sistemas protegidos, la posesión de equipos o prestación de servicios de sabotaje, el espionaje informático y la falsificación de documentos.

Por otra parte se hace referencia a lo que sería un delito informático, llegando a establecer este como una acción ilícita penada por la ley que se realiza con la ayuda de la tecnología informática en contra de soportes de sistemas técnicos de información, causando una perdida al sujeto pasivo víctima de este tipo de acciones delictivas.

En cuanto al *modus operandi* de los sujetos activos o delincuentes informáticos se llega a la conclusión que hacen uso de correos electrónicos cuyas direcciones están

disfrazada con el aparente nombre de un banco, por medio de este solicitan información personal y bancaria “supuestamente” para actualizar la base de datos de la entidad financiera: también podrá existir cámaras ocultas que permiten captar los valores digitados, el delincuente puede colocar una boquilla donde se deposita el dinero y una vez realizada la transacción bancaria, de la misma forma el punto de venta puede copiar información a un sistema para luego utilizarla y así cometer el delito informático.

Por eso, dadas las características de esta problemática, sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos. En actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.

Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los mismos, a nivel mundial se plantea el interrogante acerca de la existencia o no el delito informático.

Hay doctrinario por la tesis de la no existencia del delito informático asegurando que “Estamos en presencia de delitos clásicos en los que su naturaleza no varía en gran medida por el hecho de que para su perpetración se haga uso de moderna tecnología relacionada con la computación”.

Por lo tanto no puede hablarse de delito informático sino más bien de una categoría criminológica como delincuencia o criminalidad informática dentro de la cual se agruparán los problemas del procesamiento de datos, relevantes para el derecho penal, sin modificar los tipos penales y las conductas a ellos vinculadas. La gran mayoría de los ilícitos informáticos pueden encuadrarse en los tipos penales tradicionales, en la medida en que sistemas computarizados sean utilizados como medio, instrumento, herramienta u objeto de aquellos.

Por todo lo expuesto, debe quedar en claro el concepto en sentido amplio de Delito informático: es aquél en que se utilizan sistemas informáticos para perpetrar cualquier acción delictiva (los sistemas como nuevos medios de comisión de delitos tradicionales), y, en su terminología más estricta, es el ataque a la información (como objeto del injusto), que en su aspecto de bien inmaterial llamamos sistema o dato informático.

Formulación del problema:

¿Tiene verdadera eficacia la legislación venezolana al momento en que se cometa estos delitos informáticos?

Objetivos de la investigación

Objetivo General

Establecer una manera de que exista un buen manejo en esta área de informática por parte de un cuerpo investigativo entrenado. Es decir conjunto de técnicas empleadas para el tratamiento automático de la información por medio de sistemas computacionales.

Objetivos específicos

- Analizar si la Ley llena parcialmente el vacío legislativo en nuestro país puesto que es materia de mucha importancia.

- Analizar de los diferentes tipos de delitos informáticos

- Explicar las consecuencias y las medidas preventivas que se deben tomar en cuenta para resolver este tipo de problemas.

Alcances y limitación

Esta investigación sólo tomará en cuenta el estudio y análisis de la información referente al problema del Delito Informático, tomando en consideración aquellos elementos que aporten criterios con los cuales se puedan realizar juicios valorativos respecto al papel que juega el sistema informático ante éste tipo de hechos .No hay ninguna limitante ya que se poseen los criterios suficientes sobre la base de la experiencia de otras naciones para el adecuado análisis e interpretación de éste tipo de actos delictivos.

El tema se ha llevado a cabo tomando en cuenta las situaciones de inseguridad y delincuencia presentadas en el país y tomando en cuenta que el ordenamiento jurídico no da la posible solución a los casos y los pasos a seguir de dichas situación es necesario crear un precedente que sirva de orientación a las víctimas. En la presente investigación solo se analizan algunos aspectos sobre el delito informático. A los que está previsto en la Ley Especial contra los Delitos Informáticos.

Justificación e Importancia del Estudio

Con la presente investigación se busca asentar doctrina con respecto a la problemática que ha surgido los últimos tiempos como lo es los delitos cibernéticos, partiendo del punto del desconocimiento que existe sobre esta materia y la innegable vulnerabilidad que sufren las personas al tener acceso a internet.

El uso del internet por parte de la sociedad se hace cada vez mayor y la dependencia a estés es indudable, lo que origina que se creen mecanismo para llevar información necesaria y garantizar de esa forma la protección de los datos personales que se depositen en la web.

Los delitos informáticos evolucionan a paso agrandado, lo que conlleva al estado a idear acciones que faciliten la búsqueda, identificación, prevención y sanción de los actores y sus acciones antijurídicas.

Es necesario concientizar al pueblo sobre los mecanismos existentes para la restitución de un bien jurídico lesionado por parte de los llamados “delincuentes cibernéticos”. Es por ello que el presente informe orienta sobre las entidades, leyes, procedimientos, requisitos y formas de poner en marcha.

Sin olvidar de que se debe ajustar un poco mas a los entes encargados de recibir este tipo de denuncia debido a que hoy en día miles de personas sufren de este tipo de daño cibernéticos y al momento de exponer este tipo de denuncia no se le da alguna garantía sobre esta, para que dichos hechos no quede impune puesto a que los funcionarios encargados se toman a la ligera estos casos bien sea a nivel nacional y no les brindan protección suficiente a los ciudadanos victimas de estos delitos informáticos.

CAPITULO II

MARCO TEORICO

Antecedentes de la investigación

Los antecedentes de la investigación son los trabajos ya realizados que encuentran similitud con estudio en desarrollo. En este ámbito, a continuación se presentan las publicaciones que por su enfoque, metodología o derecho comparado su contenido sirve de referencia al tema de los delitos informáticos.

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como: robos, hurtos, fraudes, falsificaciones, perjuicios, estafas y sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha originado la necesidad de regulación por parte del derecho. Se considera que no existe una definición formal y universal de delito informático, sin embargo se han formulado conceptos respondiendo a realidades nacionales concretas.

En 1983, la Organización y Cooperación de Desarrollo Económico (OCDE) inicio un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

En 1992 la Asociación Internacional de Derecho Penal, durante el coloquio celebrado en Wurzburgo (Alemania), se adoptaron diversas recomendaciones respecto a los delitos informáticos, entre ellas que, en la medida que el Derecho Penal no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas como por ejemplo el "principio de subsidiariedad".

Se entiende Delito como: "acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria a lo establecido por aquéllas".

Finalmente la OCDE publicó un estudio sobre delitos informáticos y el análisis de la normativa jurídica en donde se reseñan las normas legislativas vigentes y se define Delito Informático como "cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos."

La lenta adecuación en Colombia del derecho penal frente a nuevas conductas derivadas del mal uso de los avances informáticos. (2012). Elaborado por: Jessica Andreina Gelvez Piza, Leidy Carolina Serrano Romero y Lina María Uribe Celis. Trabajo de Grado, Facultad de Derecho Ciencia Política y Sociales, Universidad Libre, Seccional Cúcuta. Los delitos informáticos surgen con la aparición de las computadoras, sin embargo, la legislación no ha tenido el mismo avance, especialmente en Colombia, ya que desde las décadas de los 70 y 80, muchos países han normado este importante tema, el cual en Colombia solo hasta el año 2009 mediante la ley 1273 obtuvo una importante regulación.

Es importante analizar si con la poca regulación existente en cuanto a los delitos informáticos, es posible penalizar este tipo de conductas, y si ha permitido esta normatividad que se contrarresten estas prácticas delictivas. Este trabajo analiza jurídicamente las adecuaciones que se han realizado al derecho penal colombiano, frente a las nuevas conductas derivadas del mal uso de los avances informáticos, mediante la determinación de los delitos informáticos que contempla actualmente el Código Penal Colombiano; identificando el entorno jurídico actual de las nuevas conductas derivadas del mal uso de los avances informáticos en Colombia; para finalmente demostrar si es posible con la poca normatividad penal colombiana la penalización de conductas lesivas a los sistemas informáticos.

El delito informático contra la intimidad y los datos de la persona en el derecho colombiano. (2010). Libardo Orlando Riascos Gómez. Facultad de Derecho de la Universidad de Nariño (Pasto-Colombia). El presente ensayo jurídico, titulado El delito informático contra la intimidad: una visión constitucional y penal, tiene por objeto el estudio socio jurídico del derecho fundamental a la intimidad en la Constitución y legislación penal colombiana vigente. Igualmente se hace un estudio comparado con las legislaciones penales alemana, canadiense y española, a efectos de acercarnos al análisis y tratamiento jurídicos que estas legislaciones le dan al fenómeno informático contra la intimidad.

Igualmente, hacemos un análisis detallado de los tipos penales previstos en el Código Penal Colombiano vigente (Ley 599 de 2000) y proponemos a manera de conclusión, un tipo penal complejo para proteger la intimidad de las personas que se ven ante atentados con medios comisivos electrónicos, telemáticos o informáticos o medios (TIC). Finalmente hacemos un relación de los tipos penales creados por la ley 1273 de 2009 que pretenden tutelar el bien jurídico tutelado de la "información y de los datos" personales

El material Sustraído de esta tesis fue de gran ayuda para este presente informe ya que permite especificar el tipo de delito cibernéticos que ocurren asi como las acciones que se están tomando en el exterior en cuanto a la búsqueda y tipificación de los delitos antes mencionados.

En la legislación argentina la normativa original del código penal no contemplaba la protección de la información entendida como bien intangible.

Recién a partir de la sanción de la Ley de Protección de los Datos Personales, mejor conocida como Habeas Data, (Ley N°25.326) que añadió al Código Penal los artículos 117 y 157 se le brinda protección penal a la información entendida como bien inmaterial, pero sólo cuando ésta se refiere a datos personales.

Existen otras leyes especiales que también dan tutela a ciertos intangibles, a título de ejemplo:

- La ley 24.766, llamada de confidencialidad de la información, que protege a ésta sólo cuando importa un secreto comercial;
- La ley 24.769, de delitos tributarios, que brinda tutela penal a la información del Fisco Nacional a fin de evitar su supresión o alteración.
- La ley 11.723 luego de sanción de la ley 25.036 ha extendido la protección penal al software.

  A partir del 4 de junio de 2008, la Ley 26.388 de delitos informáticos.

Teniendo en cuenta que la jurisprudencia Argentina uno de los fallos que más controversia ha generado fue el de Jorge Lanata. El periodista había sido querellado en el año 1998 por haber divulgado un email de un tercero a través de los medios. En casos similares directamente se rechazaba por atípico ya que el correo electrónico no estaba equiparado a la correspondencia epistolar y por lo tanto no contaba con protección legal.

Este fallo sentó jurisprudencia para algunas futuras presentaciones similares. El problema era que, si bien el email estaba equiparado a la correspondencia epistolar, quedaban dudas al no haber una norma que lo definiera concretamente.

Asimismo existe otro antecedente nacional en que el Juzgado Federal de Río Cuarto, el 26 de abril de 1999, desestimó una denuncia de la Universidad de Río Cuarto en un caso de acceso ilegítimo al sistema informático por no importar delito.

El acceso indebido y modificación del site de la Corte Suprema de Justicia de la Nación, es el último antecedente, y vale la pena transcribir parte del mismo:

Para el magistrado interviniente, "desde el punto de vista del derecho de fondo se debería encuadrar el hecho mencionado en la figura penal básica prevista por el artículo 183 del Código Penal, debiendo, asimismo, determinar si el mismo se encuentra

contemplado en el agravante descripto por el artículo 184 inciso 5º del mismo cuerpo legal." Cabe destacar que la primer norma citada reprime con pena de prisión de 15 días a un año al que "destruyere, inutilizare, hiciere desaparecer o de cualquier modo dañare una cosa mueble o inmueble o un animal, total o parcialmente ajeno...".

Por su parte el agravante previsto por el artículo 184 inciso 5º del Código Penal establece que la pena será de tres meses a cuatro años de prisión si el daño atípico se ejecuta "... en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público..."

Las posibles implicaciones económicas de la delincuencia informática, su carácter internacional y, a veces, incluso transnacional y el peligro de que la diferente protección jurídico-penal nacional pudiera perjudicar el flujo internacional de información, condujeron en consecuencia a un intercambio de opiniones y de propuestas de solución. Sobre la base de las posturas y de las deliberaciones la cual surgió un análisis y valoración iuscomparativista de los derechos nacionales aplicables, así como de las propuestas de reforma. Las conclusiones político-jurídicas desembocaron en una lista de las acciones que pudieran ser consideradas por los Estados, por regla general, como merecedoras de penal.

Partiendo del estudio comparativo de las medidas que se han adoptado a nivel internacional para atender esta problemática, deben señalarse los problemas que enfrenta la cooperación internacional en la esfera del delito informático y el derecho penal, a saber: la falta de consenso sobre lo que son los delitos informáticos, falta de definición jurídica de la conducta delictiva, falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, dificultades de carácter procesal, falta de armonización para investigaciones nacionales de delitos informáticos.

Adicionalmente, deben mencionarse la ausencia de la equiparación de estos delitos en los tratados internacionales. Teniendo presente esa situación, consideramos que es

indispensable resaltar que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema.

En consecuencia, es necesario que para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada. Durante la elaboración de dicho régimen, se deberán de considerar los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional.

Soto (1999) consideraciones sobre los delitos informáticos en la legislación venezolana.

En esta investigación la autora establece un estudio en las relaciones existentes entre la informática, los delitos y el derecho; de la misma establece un análisis de las distintas definiciones que la doctrina jurídica a dado a los delitos informáticos. Igualmente presenta una definición de las características de este tipo delictivo permitiendo diferenciarlo entre otros tipos penales.

Del mismo modo desarrolla los elementos de los tipos penales contenidos en la ley especial contra los delitos informáticos como: “aquellas conductas típicas, antijurídicas, y culpables que lesionan la seguridad informática de los sistemas tecnológicos y dirigidas contra bienes intangibles como datos, programas, imágenes y voces almacenadas electrónicamente”.

Del mismo modo desarrolla los elementos de los tipos penales contenidos en la ley especial contra los delitos informáticos aprobada en la República Bolivariana de Venezuela en el año 2001, considerando la seguridad jurídica como el bien jurídico tutelado por el derecho, lo que desde su punto de vista permite ampliar el conocimiento de sus diferentes manifestaciones.

Así mismo afirma que la tipificación de estas figuras delictivas era una necesidad en el país, y efectivamente se llevó a cabo, mediante la promulgación de la ley Especial contra los Delitos Informáticos.

En esta investigación tomo como objeto sentar una definición de la naturaleza de los delitos informáticos, estudiar las características de este tipo de delitos y determinar la tipificación de los delitos informáticos de acuerdo con sus características principales. Conjuntamente con ello fue analizado el impacto de estos en la vida social y tecnológica de la sociedad, asimismo también se determinaron las empresas que operan con mayor de ser víctimas de delitos informáticos

Soto (2004) análisis de diversos tipos penales contenidos en la ley especial contra los delitos informáticos venezolana.

El objeto de este tema es demostrar la importancia de los diversos tipos penales contenidos en la Ley Especial Contra los Delitos Informáticos, el bien jurídico tutelado por la doctrina penal en los delitos informáticos así como un análisis jurídico de la estructura jurídico- penal de los diversos tipos penales contenidos en la Ley Especial Contra los Delitos Informáticos aprobada en la República Bolivariana de Venezuela en el año 2001.

En Venezuela la Ley Especial Contra los Delitos Informáticos (2001) establece varios delitos que dependiendo de su origen, motivación y fin pueden clasificarse como Ciberterrorismo. El acceso indebido, el sabotaje o daño a sistemas son castigados. Se incluye como delitos la inutilización de sistemas, la creación, introducción o transmisión, por cualquier medio, virus o programas análogos. El Acceso indebido o sabotaje a sistemas protegidos por medidas de seguridad o destinados a funciones públicas o que contengan información personal o patrimonial de personas naturales o jurídicas es igualmente objeto de castigo.

Bases teórica

Para sustentar el presente trabajo investigativo, es necesario realizar una revisión documental que permita desarrollar perspectivas teóricas que contribuyan al enriquecimiento de la investigación

Nidia Callegari define al delito informático como *"aquel que se da con la ayuda de la informática o de técnicas anexas"*. Este concepto tiene la desventaja de solamente considerar como medio de comisión de esta clase de delitos a la informática, olvidándose la autora que también que lo informático puede ser el objeto de la infracción.

Davara Rodríguez define al Delito informático como, la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software.

Julio Téllez Valdés conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a *"las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin"* y por las segundas *"actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"*.

Como ya se señaló anteriormente, determinados enfoques doctrinales subrayarán que el delito informático, más que una forma específica de delito, supone una pluralidad de modalidades delictivas vinculadas, de algún modo conlos computadores.

El profesor Romeo Casabona señala que eltérmino Delito Informático debe usarse en su forma plural, en atención a que se utiliza para designar una multiplicidad de conductas ilícitas y no una sola de carácter general. Se hablará de delito informático cuando nos estemos refiriendo a una de estas modalidades en particular.

El Doctor Gabriel A. Cámpoli los delitos informáticos aparece como un mundo que puede decirse no al alcance de la mayoría y más aún si nos adentramos específicamente en el punto de los delitos electrónicos ya que su aprehensión implica un mayor grado de compromiso con conocimientos tecnológicos resultan sólo para algunos elegidos.

María de la Luz Lima, dice que el *"delito informático en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea con método, medio o fin".*

Según Messina (1989) el derecho informático es el conjunto de normas, reglas y principios jurídicos que tienen por objeto evitar que la tecnología pueda conculcar derechos fundamentales del hombre y que se ocupa de la regulación de lo relativo a la instrumentación de las nuevas relaciones jurídicas derivadas de la producción y uso de los bienes informáticos, así como de la transmisión de datos.

El derecho informático es una ciencia que constituye un conjunto de normas, aplicaciones, procesos, relaciones jurídicas que surgen como consecuencia de la aplicación y desarrollo de la informática y su aplicación en todos los campos. Se podría definir también el derecho informático como la ciencia que estudia la regulación normativa de la informática.

Zabale, define los delitos informáticos como: *"toda conducta que revista característica delictivas, es decir sea típica, antijurídica y culpable y atente contra el soporte lógico de un sistema de procesamiento de información, sea sobre programas o datos relevantes, a través del empleo de las tecnologías de la información y el cual se distingue de los delitos computacionales o tradicionales informatizados"*.

Pérez citado por Montoya (1999) define *"que la informática jurídica es el procesamiento automático de información jurídica* "es el tratamiento automatizado de

las fuentes de conocimientos jurídicos (sistemas de documentación legislativa, jurisprudencial y doctrinal), de las fuentes de producción jurídica y su organización (funcionamiento de organismos legislativo y judicial) y de las decisiones judiciales.

Flores (2009) los delitos informáticos son toda acción (acción u omisión) culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, tipificando por la ley, que se realiza en el entorno informático y está sancionado con una pena.

Bases Legales

En este punto se muestran las normas que constituyen el marco legal para el presente trabajo de investigación, en este sentido dentro del ordenamiento Jurídico Venezolano lo sustentan las siguientes normas:

Dentro de este esfuerzo que se ha venido dando, tanto en el ámbito interno de cada país como a nivel internacional para perseguir los delitos informáticos nos encontramos ante el caso de Venezuela que en los últimos cuatro años ha comenzado a legislar sobre este tema.

En Venezuela comenzó con la aprobación de la **Constitución de la República Bolivariana de Venezuela, que establece en su artículo 110 lo siguiente:**

Artículo 110.

> *"El Estado reconocerá el interés público de la ciencia, la tecnología, el conocimiento, la innovación y sus aplicaciones y los servicios de información necesarios por ser instrumentos fundamentales para el desarrollo económico, social y político del país, así como para la seguridad y soberanía nacional. Para el fomento y desarrollo de esas actividades, el Estado destinará recursos suficientes y creará el sistema nacional de ciencia y tecnología de acuerdo con la ley. El sector privado deberá aportar recursos para los mismos. El Estado garantizará el cumplimiento de los principios éticos y legales que deben regir las actividades de investigación científica, humanística y tecnológica. La ley determinará los modos y medios para dar cumplimiento a esta garantía"*.

Ley Especial contra los delitos informáticos, Gaceta oficial Nº 37.313 de fecha 30 de octubre de 2001 (entrada en vigencia 2002).

Esta novísima Ley contra Delitos Informáticos, aprobada a finales del año 2001, significa un gran avance en materia penal para mi país, visto que nos permitirá la protección de la tecnología de la información, persiguiendo todas aquellas conductas antijurídicas que se realicen en este campo. Es por eso, que a continuación señalare los aspectos más importantes de la ley:

Objeto de la Ley.

El objeto de la Ley se encuentra consagrado en el artículo 1 el cual establece:

Artículo 1.

> *"La presente ley tiene por objeto la protección de los sistemas que utilicen tecnologías de información, así como la prevención y sanción*

de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley."

Artículo 2. Definiciones. A efectos de la presente Ley, y cumpliendo con lo previsto en el artículo 9 de la Constitución de la República Bolivariana de Venezuela, se entiende por:

Tecnología de Información: *rama de la tecnología que se dedica al estudio, aplicación y procesamiento de datos, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, transmisión o recepción de información en forma automática, así como el desarrollo y uso del "hardware", "firmware", "software", cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de datos***.**

Extraterritorialidad.

La previsión de la Extraterritorialidad se encuentra señalado en su artículo 3, y el cual es de gran importancia en razón de la dimensión transnacional del problema pues se trata de hechos que pueden cometerse de un país a otro es por eso que en el articulo establece:

Artículo 3. Extraterritorialidad.

Cuando alguno de los delitos previstos en la presente Ley se cometa fuera del territorio de la República, el sujeto activo quedará sometido a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible, y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.

Sanciones.

Artículo 4. Sanciones.

> *Las sanciones por los delitos previstos en esta Ley serán principales y accesorias. Las sanciones principales concurrirán con las penas accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito del cual se trate, en los términos indicados en la presente Ley.*

Para las sanciones se adoptó simultáneamente el sistema binario, esto es, pena privativa de libertad y pena pecuniaria. Con relación a esta última se fijan montos representativos calculados sobre la base de unidades tributarias por considerarse que la mayoría de estos delitos, no obstante la discriminación de bienes jurídicos que se hace en el proyecto, afecta la viabilidad del sistema económico, el cual se sustenta, fundamentalmente, en la confiabilidad de las operaciones. Cabe destacar que el legislador tomó en cuenta las deficiencias de otras leyes donde no se preveían las penas accesorias. Así, en la ley encontramos que las penas para los hechos punibles que se encuentran tipificados son principales y accesorias.

Se establece como penas accesorias las siguientes:

- *El decomiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que haya sido utilizado para la comisión de los delitos.*
- *El trabajo comunitario.*
- *La inhabilitación para el ejercicio de funciones o empleos públicos, para el ejercicio de la profesión industria, o para laborar en instituciones o empresas del ramo.*

- *La suspensión del permiso, registro o autorización para operar el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información.*
- *Divulgación de la sentencia condenatoria.*
- *Indemnización civil a la víctima por los daños causados.*

Clasificación de los Delitos Informáticos.

La ley clasifica los delitos informáticos de acuerdo al siguiente criterio:

1) **Delitos contra los sistemas que utilizan tecnologías de Información:**

Artículo 6. Acceso indebido.

Toda persona que sin la debida autorización Excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información, será penado con prisión de uno a cinco años multa de diez a cincuenta unidades tributarias.

Artículo 7. Sabotaje o daño a sistemas.

Todo aquel que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera de los componentes que lo conforman, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Artículo 8. Favorecimiento culposo del sabotaje o daño.

Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o Inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios.

Artículo 9. Acceso indebido o sabotaje a sistemas protegidos.

Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad, cuando los hechos allí previstos o sus efectos recaigan sobre cualesquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.

Artículo 10. Posesión de equipos o prestación de servicios de sabotaje.

Quien importe, fabrique, distribuya, venda o utilice equipos, dispositivos o Programas, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información; o el que ofrezca o preste servicios destinados a cumplir los mismos fines, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Artículo 11. Espionaje informático.

Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penada con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado.

Artículo 12. Falsificación de documentos.

Quien, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

2) Delitos contra la propiedad.

Artículo 13. Hurto.

Quien a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 14. Fraude.

Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

Artículo 15. Obtención indebida de bienes o servicios.

Quien, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice

indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio; o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 16. Manejo fraudulento de tarjetas inteligentes o instrumentos análogos.

Toda persona que por cualquier medio cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o la persona que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema, con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía de éstos, será penada con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias.

En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o dela data o información contenidas en ellos o en un sistema.

Artículo 17. Apropiación de tarjetas inteligentes o instrumentos análogos.

Quien se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se haya perdido, extraviado o que haya sido entregado por equivocación, con el fin de retenerlo, usarlo, venderlo o transferirlo a una persona distinta del usuario autorizado o entidad emisora, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias. La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo.

Artículo 18. Provisión indebida de bienes o servicios.

Todo aquel que, a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado; se haya indebidamente obtenido, retenido, falsificado, alterado; provea a quien los presente de dinero, efectos, bienes o servicios, o cualquier otra cosa de valor económico será penado con prisión de dos seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 19. Posesión de equipo para falsificaciones.

Todo aquel que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines, o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

3) Delitos contra la privacidad de las personas y de las comunicaciones.

Artículo 20. Violación de la privacidad de la data o información de carácter personal.

Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que

utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas seiscientas unidades tributarias.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Artículo 21. Violación de la privacidad de las comunicaciones.

Toda persona que mediante el uso de tecnologías de información acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 22. Revelación indebida de data o información de carácter personal.

Quien revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidas por alguno de los medios indicados en los artículos 20 y 21, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

4) Delitos contra niños, niñas o adolescentes.

Artículo 23. Difusión o exhibición de material pornográfico.

Todo aquel que, por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 24. Exhibición pornográfica de niños o adolescentes.

Toda persona que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penada con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

5) Delitos contra el orden económico.

Artículo 25. Apropiación de propiedad intelectual.

Quien sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

Artículo 26. Oferta engañosa.

Toda persona que ofrezca, comercialice o provea de bienes o servicios, mediante el uso de tecnologías 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.

Como puede apreciarse en Venezuela se ha dado un paso importante en la legislación penal que regula los delitos informáticos pero que debe continuar con su evolución para enfrentar las exigencias de un mundo en proceso de globalización.

En cuanto al código de procesal penal venezolano tenemos presente el siguiente artículo:

Artículo 120 de la víctima.

> *La protección y reparación del daño causado a la víctima del delito son objetivos del proceso penal. El ministerio público está obligado a velar por dichos intereses en todas las fases. Por su parte, los jueces y juezas garantizaran la vigencia de sus derechos y el respeto, protección y reparación durante su proceso.*

Articulo 223 experticias.

> *El ministerio realizara u ordenara la práctica de experticias cuando para el examen de una persona u objeto, o para descubrir o valorar un elemento de convicción, se requieran conocimiento o habilidades especiales en alguna ciencia, arte u oficio.*
>
> *El o la fiscal del ministerio público, podrá señalarse a los o las peritos asignados, el aspecto más relevante que deben ser objeto de la peritación, sin que esto sea limitativo, y el plazo dentro del cual presentara su dictamen.*

Definición de términos básicos

- **Antijurídica:** es uno de los elementos considerados por la teoría del delito para la configuración de un delito. Se le define como aquel desvalor que posee un hecho típico que es contrario a las normas del Derecho.

- **Criminalidad informática:** según la RAE son actos económicos criminales con el uso de ordenadores o sistemas de comunicación. En sentido amplio, es todo delito que implique la utilización de cualquier medio de tecnología informática. La conducta antijurídica, culpable y punible, se vale de medios tecnológicos para la comisión del delito.

- **Ciberterrorismo:** en el diccionario jurídico define que el ciberterrorismo o terrorismo electrónico es el uso de medios de tecnologías de información, comunicación, informática, electrónica o similar con el propósito de generar terror o miedo generalizado en una población, clase dirigente o gobierno, causando con ello una violación a la libre voluntad de las personas.

- **Daño:** Daño pueden definirse como el deterioro, menoscabo o destrucción cuyo perjuicio patrimonial es evaluable económicamente. La delimitación del concepto radica en la asistencia de un conjunto de elementos propios y específicos que han de configurarse dentro de un amplio y genérico compendio desde que la acción punible de dañar se corresponda con los términos cuya definición correspondan como la pérdida total o parcial, y pérdida de su eficacia, productividad o rentabilidad

- **Datos:** según el diccionario jurídico se conoce que la palabra Datos proviene del latín “Dtum” cuyo significado es “lo que se da”. Los datos son la representación simbólica, bien sea mediante números o letras de una recopilación de información la cual puede ser cualitativa o cuantitativa, que facilitan la deducción de una investigación o un hecho.

- **Espionaje**: según la RAE Los programas de espionaje informático envían informaciones del computador del usuario de la red para desconocidos. Hasta lo que es digitado en su teclado puede ser monitoreado por ellos. Algunos tienen un mecanismo que hace una conexión con el servidor del usuario siempre que el estuviera conectado on-line.

- **Falsificación:** Falsificación de un instrumento financiero, significa una persona a sabiendas y voluntariamente falsificado, espuria, en relieve, o codificados magnéticamente o electrónicamente cualquier tarjeta de las transacciones financieras, giro postal o cheque.

- **Firmware:** es un soporte lógico inalterable es un programa informático que establece la lógica de más bajo nivel que controla los circuitos electrónicos de un dispositivo de cualquier tipo. En resumen, un firmware es un software que maneja físicamente al hardware.

- **Gusanos:** Un gusano informático es un malware que tiene la propiedad de duplicarse a sí mismo. Los gusanos utilizan las partes automáticas de un sistema operativo que generalmente son invisibles al usuario.

- **Hardware:** En informática, se denomina hardware o soporte físico al conjunto de elementos materiales que componen un computador. Hardware también son

los componentes físicos de una computadora tales como el disco duro, la unidad de disco óptico, la disquetera, etc.

- **Instrumento:** son programas, aplicaciones o simplemente instrucciones usadas para efectuar otras tareas de modo más sencillo. En un sentido amplio del término, podemos decir que una herramienta es cualquier programa o instrucción que facilita una tarea.

- **Información:** La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento.

- **Microprocesadores:** El microprocesador (o simplemente procesador) es el circuito integrado central más complejo de un sistema informático; a modo de ilustración, se le suele llamar por analogía el «cerebro» de un ordenador.

- **Miniaturización**: Según la RAE se denomina miniaturización al proceso tecnológico mediante el cual se intenta reducir el tamaño de los dispositivos electrónicos.

- **Protección:** según la RAEL la seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

- **Sabotaje:** El término sabotaje informático comprende todas aquellas conductas dirigidas a eliminar o modificar funciones o datos en una computadora sin

autorización, para obstaculizar su correcto funcionamiento, es decir, causar daños en el hardware o en el software de un sistema.

- **Software:** Se conoce como software al soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

CAPITULO III

MARCO METODOLOGICO

En esta sección se exponen de forma precisa el tipo de datos que se requiere indagar para el logro de los objetivos de la investigación, así como la descripción de los distintos métodos y las técnicas que posibilitan obtener la información necesaria.

Tipo de investigación

En la presente investigación es de tipo documental. Según Fidias G. arias (2002)

La investigación documental es un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, es decir, los obtenidos y registrados por otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas. Como en toda investigación, el propósito de este diseño es el aporte de nuevos conocimientos.

Como parte esencial de un proceso de investigación documental, puede definirse también como una estrategia de la que se observa y reflexiona sistemáticamente sobre realidades teóricas y empíricas usando para ello diferentes tipos de documentos donde se indaga, interpreta, presenta datos e información sobre un tema determinado de cualquier ciencia, utilizando para ello, métodos e instrumentos que tiene como finalidad obtener resultados que pueden ser base para el desarrollo de la creación científica

Así mismo, considerando los objetivos propuesto en la presente investigación es un proyecto por el cual se plantea la importancia de los delitos informáticos a nivel nacional

e internacional esto con el fin de lograr proteger las pertenencias e integridad de los usuarios. Se busca resolver una problemática que es indispensable hoy en día en la población.

Métodos y técnicas de investigación jurídica

Miriam Balestrini (p.131) nos señala que: “un diseño de investigación se define se define como el plan global de investigación que integra de un modo coherente y adecuadamente correcto técnicas de recogidas de datos a utilizar, análisis previstos y objetivos”.

Todo proceso de investigación requiere de un diseño que oriente la construcción y aplicación de un instrumental que permita la recolección de datos e información para su posterior tratamiento. Ello implica la previsión de los pasos que ha de seguir para lograr los objetivos de la investigación y asimismo detallar la forma en cómo la información requerida va a ser extraída y como ella será transformada en información.

Fases de investigación

Según el autor (Santa palella y feliberto Martins (2010), define: La investigación documental se concreta exclusivamente en la recopilación de información en diversas fuentes. Indaga sobre un tema en documentos-escritos u orales- uno de, los ejemplos más típicos de esta investigación son las obras de historia.

La investigación es un proceso por el cual va dirigido en buscar la solución a problemas mediantes conocimientos. Este proceso consiste en tres fases metodológicas que van en concordancia con los objetivos específicos los cuales son los siguientes:

Fase I. Analizar si la Ley llena parcialmente el vacío legislativo en nuestro país puesto que es materia de mucha importancia. (Acevedo, 2010), "Los delitos informáticos son aquellas actividades ilícitas que se cometen mediante el uso de computadoras, sistemas informáticos u otros dispositivos de comunicación (la informática es el medio o instrumento para realizar un delito) o Tienen por objeto causar daños, provocar pérdidas o impedir el uso de sistemas informáticos".

En es esta fase se buscar analizar y estudiar de forma completa la ley especial contra delitos informáticos con la finalidad de determinar el alcance y su ámbito que tiene para cubrir todo los supuestos de hechos y su ámbito de aplicación que surjan en relación a los delitos cibernéticos.

Fase II. Analizar los diferentes tipos de delitos informáticos. Esta fase pertenece a la investigación documental, según Franklin (1997) define la investigación documental aplicada como una técnica de investigación en la que se "se debe seleccionar y analizar aquellos escritos que contienen datos de interés relacionados con el estudio".

En esta fase se busca determinar los tipos de delitos informáticos que existen en la ley especial, su composición o estructura, métodos utilizados para su cumplimiento o métodos utilizados para ejecutarlos; así como el mecanismo que puedan emplearse para prevenir y sancionar

Fase III. Explicar las consecuencias y las medidas preventivas que se deben tomar en cuenta para resolver este tipo de problemas.

En esta fase busca analizar los delitos para explicar las consecuencias jurídicas que conllevan, así como los métodos y procedimientos empleados para darle solución a los conflictos que se crean en la comisión de estos actos antijurídicos.

Fuentes de conocimientos jurídicos

En este proyecto las fuentes que se utilizaron fueron los siguientes:

- Constitución de la república bolivariana de Venezuela.
- Ley especial contra los delitos informáticos.
- Código orgánico procesal penal.

CAPITULO IV

Resultados, Conclusiones y Recomendaciones.

Resultados

Los resultados de la presente investigación se relacionan con el análisis construido por los autores acorde a los objetivos planteados en el primer capítulo de dicha investigación y conforme a la apreciación personal creada de acuerdo al estudio realizado en la legislación, la doctrina tanto nacional como internacional y la jurisprudencia revisada para tales fines.

En Venezuela en cada momento se hace presente la posibilidad de estos delitos informáticos producto de la situación política, económica y escasa seguridad social. Por tal sentido fue creada en Gaceta oficial Nº 37.313 de fecha 30 de octubre de 2001 (entrada en vigencia 2002) la ley especial contra los delitos informáticos.

Estudio de las acciones típicas del delito informático

En este contexto los primeros resultados a plantear son los que se desprendieron del primer objetivo de la investigación, en el cual se refirió a: “Analizar si la Ley llena parcialmente el vacío legislativo en nuestro país puesto que es materia de mucha importancia”.

En este sentido se debe acotar que este tipo delictivo habitualmente se realiza con el fin de obtener un beneficio o provecho personal que generalmente es económico provocando así un perjuicio o daño patrimonial al titular de cuenta, quien es el sujeto pasivo y que la mayoría de las veces sin que este se percate del delito del cual está siendo víctima.

Es necesario un análisis sobre el tema de los delitos informáticos, ya que son escasos los textos y la información que se encuentra en la red sobre este tema. Especialmente en Venezuela se redacta muy poco sobre la materia y cabe resaltar que este tipo de tema se estudian por interés académico o por la necesidad de resolver un problema de cual hemos sido víctimas ya sea por estafa en compra de un artículo por medio del internet, engaños en la red, manipulación de información en las bases de datos de los sistemas, aun cuando Venezuela carece en gran medida de conocimientos sobre el internet más la ley especial antes mencionada y sus peligros más que en sus beneficios, podemos mencionar que se ha comenzado a dar importancia al tema de delitos informáticos.

Sin olvidar que hoy en día se debe tener en cuenta también el manejo correcto por parte de las autoridades que manejan este tipo de delitos. Actualmente en Venezuela se cuenta con un grupo especializado dentro del Cuerpo de Investigaciones Científicas, Penales y Criminalísticas (CICPC), llamado División de Delitos Informáticos. Donde podemos acudir si somos víctimas de un chantaje, estafa o robo de información electrónica entes encargados y especializados en esta clase de crímenes.

Es importante tener el conocimiento donde denunciar, ya que en los últimos años se está utilizando la creación de perfiles o formularios falsos en las cuales contiene publicidad engañosa donde anuncia premios, viajes o promociones. Esta modalidad es muy utilizada para los delincuentes del ciberespacio ya que el usuario de forma voluntaria registra sus datos; y así obtener datos valiosos y necesarios para cometer los delitos como son nombre, apellido, cedula, tarjetas, correo, password y pare de contar.

Para evitar ser engañados, debemos estar alerta porque cada vez que avanza la tecnología, crecen los delitos informáticos, para que el sistema surta sus efectos en necesario concientizar a la población para que los usuarios de la tecnología sean más responsables y consientes a la hora de suministrar datos bien sea personales o bancarios, unas de las recomendaciones que podemos dar es a la hora de recibir un correo con virus o que están en la bandeja de spam no reenviarlos, ya que que de esta manera podrían al

hacerlos paralizar los sistemas u ocasionar perdidas de información o extracción de información.

Se debe ser entradamente cuidadoso a la hora de colocar los datos en la red, ya que existen personas que se dedican a buscar estos tipos de información con el objetivo de utilizarlos en la elaboración de planes; bien sea para secuestrar, extorsionar y causar daños morales y psicológicos.

La doctrina ha determinado que el elemento de culpabilidad es aplicable al sujeto activo de hecho punible ya que al cometer la actividad delictiva el sujeto busca un beneficio propio o de un tercero que mayoritariamente es de aspecto económico. Ocasionándole un perjuicio al sujeto pasivo, que en este tipo delictivo puede ser una persona jurídica ya sea como bancos, establecimientos, comerciales, etc. la administración pública o una persona natural.

El sujeto activo de esta clase de infracciones puede ser totalmente anónimo y usar este anonimato como forma de evadir su responsabilidad, ya que este no necesariamente puede usar su propio sistema informático, sino que se puede valer de un tercero,en el cual se puede usar a una máquina zombi, es decir una computadora que está bajo el control del SPAMER y que le permite usarla como una estación de trabajo de su propia red de máquinas zombis, las cuales pertenecen a usuarios desaprensivos que no tienen al día sus medidas de seguridad y que son fácil presa de los hackers y crakers para cometer este tipo de infracciones. También existen programas de enmascaramiento o que no permiten ver la verdadera dirección ya sea de correo electrónico o del numero IP.

Conclusiones

Venezuela debería trabajar con nuevas plataformas tecnológicas y un equipo de investigación completamente entrenado en el tema, para que de esta manera sea más fácil detectar ataques o sabotajes cibernéticos, como resultado de la investigación, es posible concluir que en Venezuela existen distinto tipos de delitos informáticos, y en los últimos años surgieron nuevas alternativas que ayudaran a que estos delitos no quede impune, por esta razón se promulgo la nueva ley contra delitos informáticos, la cual permite un mejor manejo de las pruebas o evidencias digitales.

Se considera que los organismo del estado, los cuales le compete tomar verdaderas medidas disciplinarias para que los ciudadanos no incurran en este tipo de delitos; deben reforzar sus mecanismo de detección e implementar equipos tecnológicos más avanzados y cuerpo investigativo adecuado, debido a que constituye un reto enorme para para dichas autoridades, investigadores y funcionarios judiciales.

Los cuales son responsables de aplicar las sanciones a quienes incurran en los delitos, independientemente del rango político, económico e institucional que tenga dentro del estado venezolano.

Debido a la naturaleza virtual de los delitos informáticos, puede volverse confusa la tipificación de estos delitos ya que a nivel general, se poseen pocos conocimientos y experiencias en el manejo de ésta área. Desde el punto de vista de la Legislatura es difícil la clasificación de estos actos, por lo que la creación de instrumentos legales puede no tener los resultados esperados, sumado a que la constante innovación tecnológica obliga a un dinamismo en el manejo de las Leyes relacionadas con la informática.

La falta de cultura informática es un factor crítico en el impacto de los delitos informáticos en la sociedad en general, cada vez se requieren mayores conocimientos en

tecnologías de la información, las cuales permitan tener un marco de referencia aceptable para el manejo de dichas situaciones.

Al dar a conocer los distintos delitos informáticos en la tecnología, la sociedad comprenderá un punto de vista diferente, por el cual tendrá más cuidado al dar información confidencial y habrá menos fraudes electrónicos, ya que no cualquier persona hará compras electrónicas en cualquier sitio web de compras, solo en sitios de prestigio y garantizados.

Recomendaciones

Fase I

- **Actualizar regularmente los sistemas operativo** y el software instalado en los equipo, poniendo especial atención a las actualizaciones en el navegador web. A veces, los sistemas operativos presentan fallos, que pueden ser aprovechados por delincuentes informáticos.

  Frecuentemente aparecen actualizaciones que solucionan dichos fallos. Estar al día con las actualizaciones, así como aplicar los parches de seguridad recomendados por los fabricantes, se ayudará a prevenir la posible intrusión de hackers y la aparición de nuevos virus.

- **Instalar un Antivirus y actualizar con frecuencia**. Analizar con un antivirus todos los dispositivos de almacenamiento de datos que se utilicen y todos los archivos nuevos, especialmente aquellos archivos descargados de internet.

- **Instalar un Firewall o Cortafuegos** con el fin de restringir accesos no autorizados de Internet.

- **Es recomendable tener instalado en su equipo algún tipo de software anti-spyware**, para evitar que se introduzcan en su equipo programas espías destinados a recopilar información confidencial sobre el usuario.

Fase II

- **Utilice contraseñas seguras**, es decir, aquellas compuestas por ocho caracteres, como mínimo, y que combinen letras, números y símbolos. Es

conveniente además, que modifique sus contraseñas con frecuencia. En especial, le recomendamos que cambie la clave de su cuenta de correo si accede con frecuencia desde equipos públicos.

- **Navegue por páginas web seguras y de confianza**. Para diferenciarlas identifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. Extreme la precaución si va a realizar compras online o va a facilitar información confidencial a través de internet. En estos casos reconocerá como páginas seguras aquellas que cumplan dos requisitos:
  - Deben empezar por https:// en lugar de http.
  - En la barra del navegador debe aparecer el icono del candado cerrado. A través de este icono se puede acceder a un certificado digital que confirma la autenticidad de la página.

- **Sea cuidadoso al utilizar programas de acceso** remoto. A través de internet y mediante estos programas, es posible acceder a un ordenador, desde otro situado a kilómetros de distancia. Aunque esto supone una gran ventaja, puede poner en peligro la seguridad de su sistema.

- **Ponga especial atención en el tratamiento de su correo electrónico**, ya que es una de las herramientas más utilizadas para llevar a cabo estafas, introducir virus, etc.
- No abra mensajes de correo de remitentes desconocidos.
- **Desconfíe de aquellos e-mails** en los que entidades bancarias, compañías de subastas o sitios de venta online, le solicitan contraseñas, información confidencial, etc.
- **No propague aquellos mensajes de correo con contenido dudoso** y que le piden ser reenviados a todos sus contactos. Este tipo de mensajes, conocidos

como hoaxes, pretenden avisar de la aparición de nuevos virus, transmitir leyendas urbanas o mensajes solidarios, difundir noticias impactantes, etc.

- **Utilice algún tipo de software Anti-Spam** para proteger su cuenta de correo de mensajes no deseados. En general, es fundamental estar al día de la aparición de nuevas técnicas que amenazan la seguridad de su equipo informático, para tratar de evitarlas o de aplicar la solución más efectiva posible.

Fase III

- **Haz una copia de la información**. a manera de prevención, luego de que hayas realizado tu compra imprime la orden de transacción y la página pues ésta contiene el nombre del negocio, la dirección, el número telefónico y los términos legales de tu compra (no olvides asegurarte previamente de que toda la información del negocio sea verdadera).

- **Delitos comunes** Los delitos más comunes en internet son el fraude, extorsión, amenazas, pornografía y la trata de personas. la mayoría de éstos delitos ocurre debido al exceso de información personal que detallas tú o los niños en sus redes sociales o en otras páginas web; evita agregar tus datos personales, dirección o mostrar imágenes que de alguna manera hagan alusión a tu nivel socioeconómico y supervisa el uso que hacen del internet los niños.

- **Denúncialo** estima que del total de delitos informáticos en Venezuela es poco denunciado, lo cual de alguna manera permite que los ciberdelitos se sigan multiplicando. para realizar la denuncia debes acudir al CICPCy ministerio público y rendir tu declaración de los hechos, puedes agregar pruebas como

los correos de la conversación, el depósito realizado, nombre y teléfono de la cuenta del defraudador y el nombre de la empresa o comercio en el cual compraste el artículo.

Fase IV

- **No abrir ficheros adjuntos sospechosos**. Si es de un conocido hay que asegurarse de que realmente lo quiso enviar. Los virus utilizan esta técnica para propagarse entre los contactos del correo, así como los contactos de la mensajería instantánea y de las redes sociales.

- **Pensar antes de publicar**. Los servicios actuales de Internet facilitan las relaciones sociales, lo que conlleva a su vez se publiquen mucha información sobre las personas (datos personales, imágenes, gustos, preferencias, etc.).

  Dado el valor que tiene esta información, y las repercusiones negativas que puede tener su uso inadecuado por parte de otras personas, es necesario que se gestionen adecuadamente.

- **Conocer los riesgos asociados al uso de Internet**. ¡Hay que mantenerse al día! Es aconsejable estar suscrito a páginas que informen sobre estos delitos.

REFERENCIAS BIBLIOGRÁFICAS

- Constitución de la República Bolivariana de Venezuela (1999) Gaceta Oficial Nº 5.453 de fecha 24 de marzo del 2000.

- Ley Especial Contra los Delitos Informáticos, Gaceta Oficial Nº37.313 de fecha 30 de octubre de 2001.

- Código orgánico procesal penal, Decreto Nº 9.042 de fecha de 12 de junio del 2012.

- Artega S., Alberto. El delito informático: algunas consideraciones jurídico penales Revista de la Facultad de Ciencias Jurídicas y Políticas. No. 68 Año 33. Universidad Central de Venezuela. 1987. Caracas, Venezuela.

- Estrada Garavilla Miguel. Revista de delitos informáticos, universidad abierta.

- Yann derrien *DELITOS INFORMATICOS 2da edición 1982-1989.*

- José Anotnio Echenique *seguridad informatica2000.*

- Leal almado, análisis de delitos y manejos de sistemas informáticos o instrumentos en el ordenamiento jurídico venezolano.

- DR. Santiago Acurio del Pino, delitos informáticos: generalidades.