UNIVERSIDAD JOSÉ ANTONIO PÁEZ

La Vulnerabilidad Jurídica en materia Penal Informática y su Escasa Regulación dentro del Marco Legal Venezolano

Autor(es)

Sánchez R. Víctor A. C.I.: 27.097.544

Tovar V. Johely A. C.I.: 29.569.376

Urb. Yuma II, calle N°3, Municipio San Diego

Teléfono (0241) 8714240 (máster) – Fax (0241) 8712394

REPÚBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JOSÉ ANTONIO PÁEZ

FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS

ESCUELA DE DERECHO.

La Vulnerabilidad Jurídica en materia Penal Informática y su Escasa Regulación dentro del Marco Legal Venezolano

Proyecto de Trabajo de grado para optar al título de Abogado

Autor(es):

Sánchez Reyes, Víctor Alexander

Tovar Veloz, Johely Andrea

Tutor: Abg. German Brea.

San Diego, Diciembre 2021

UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS
ESCUELA DE DERECHO
COORDINACIÓN DE PASANTÍA Y TRABAJO DE GRADO

ACTA DE APROBACIÓN

INFORME FINAL DE PASANTÍA ☐

TRABAJO DE GRADO [X]

El jurado designado por la Facultad de Ciencias Jurídicas y Políticas para la evaluación del Trabajo de Grado titulado: **"LA VULNERABILIDAD JURÍDICA EN MATERIA PENAL INFORMÁTICA Y SU ESCASA REGULACIÓN DENTRO DEL MARCO LEGAL VENEZOLANO "** realizado por los bachilleres: Sánchez Reyes, Víctor, C.I N° 27.097.544 y Tovar Veloz, Johely, C.I N° 29.569.376, cursantes de la carrera de Derecho, hace constar después de analizar su contenido y oída la exposición oral, considera que el Trabajo de Grado ha obtenido la calificación de:

APROBADO [X] NO APROBADO ☐

El Jurado;

Tutor Académico:
Prof. Brea, Germán
C.I: 6.403.553

Jurado:
Prof. Méndez, Teresa.
C.I: 5.061.814

Jurado:
Prof. Silva, Marina.
C.I: 7.332.513

Fecha: 20 de enero 2022

REPÚBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JOSÉ ANTONIO PÁEZ

FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS

ESCUELA DE DERECHO

La Vulnerabilidad Jurídica en materia Penal Informática y su Escasa Regulación dentro del Marco Legal Venezolano

Autor (es): Sánchez R, Víctor A.

Tovar V, Johely A.

Tutor (a): Abg. German Brea.

Fecha: Diciembre 2021

RESUMEN INFORMATIVO

La presente investigación tiene como propósito estudiar la vulnerabilidad jurídica en materia penal informática y su escasa regulación dentro del marco legal venezolano, cuya importancia deriva del increíble desarrollo de la tecnología, el cual ha abierto las puertas a nuevas posibilidades de delitos antes inimaginables, como la manipulación fraudulenta de los ordenadores con ánimos de lucro, la destrucción de programas o datos y, el acceso y la utilización indebida de la información, lo cual afecta la esfera de la privacidad. Es por ello que, a través de una investigación jurídica de tipo bibliográfico, citada en la investigación documental de nivel descriptivo, y desarrollándose dentro de la línea de investigación del Sistema Penal y la Administración de Justicia, mediante las técnicas bibliográficas y audiovisuales; se logró concluir que cada cierta década el Derecho Penal se ve superado por la realidad, realidad que indica su desactualización como protector social y la necesidad de una reforma.

Descriptores: Ciberdelincuencia, Derecho penal informático, Escasa regulación, Marco legal venezolano, Privacidad, Vulnerabilidad jurídica.

DEDICATORIA

A Dios por permitirnos llegar hasta aquí, y darnos la sabiduría necesaria para culminar con éxitos nuestra carrera universitaria.

A nuestros padres por ser apoyo y motivación, por estar al pendiente de nuestros estudios y dar lo mejor de ellos para que nosotros seamos buenas personas.

A nuestros hermanos, por ser apoyo y estar presente en los buenos y malos momentos, esperamos que les sirva como ejemplo de constancia y dedicación.

A nuestros abuelos, por esperar con ansias nuestro título como Abogados de la Republica.

A nuestro tutor por guiarnos y compartir sus conocimientos con nosotros. Y a cada uno de los profesores de la Universidad José Antonio Páez que nos enseñaron con dedicación, amor y vocación durante cada semestre.

A las maravillosas personas que conocimos durante estos años y que de una u otra forma nos ayudaron a lograr esta meta.

Y por supuesto, a nuestra Alma Máter, Universidad José Antonio Páez, por acogernos entre su gremio estudiantil, motivarnos a la excelencia e inculcarnos La Pasión por el Saber.

AGRADECIMIENTO

Usamos estas líneas para agradecer principalmente a Dios por darnos fuerza para continuar en este proceso de lograr una de nuestras metas.

A nuestros padres por su amor, trabajo y sacrificio en todos estos años, gracias a ustedes hemos logrado llegar hasta aquí y convertirnos en lo que somos.

A nuestro tutor, abogado y profesor German Brea, por la guía y orientación brindada durante la elaboración de la presente investigación.

Agradecemos a nuestros profesores de la Facultad de Ciencias Jurídicas y Políticas de la Universidad José Antonio Páez por haber compartido sus conocimientos a lo largo de la preparación de nuestra profesión.

A todos las personas que nos han apoyado y han hecho que el trabajo se realice con éxito, en especial a aquellos que nos abrieron las puertas y compartieron sus conocimientos.

Tovar, J.

Sánchez, V.

INDICE GENERAL

Pág.

INTRODUCCION

A medida que aumenta la ciberdelincuencia, varios países han promulgado leyes declarando ilegales nuevas prácticas, considerando delito informático algunos como “la piratería informática” o han actualizado leyes obsoletas para que los delitos tradicionales como el fraude se consideren ilegales dentro del mundo virtual. Todo esto ya que, se busca acercarse lo más posible a los distintos medios de protección para salvaguardar la información, cuyo peligro inminente se produce de acuerdo al uso que se le dé a la misma.

En Venezuela, la escasa regulación que existe con respecto a los delitos informáticos ha generado diversas acciones negativas en lo que respecta al área del Derecho Penal informático, acciones que no están previstas dentro del ordenamiento jurídico venezolano vigente, lo que convierte al país en un paraíso para la comisión de actos que perjudican o agreden los bienes jurídicos tutelados por el Estado.

Ahora bien, el bien jurídico atacado por la ciberdelincuencia es, precisamente, la información, en todos sus aspectos; información que tendrá la importancia que los poseedores le otorguen, y en términos generales, este fenómeno se podría distinguir de los otros delitos ya que no tiene barrera físicas o geográficas, y se puede cometer con más facilidad y rapidez que los delitos comunes. Teniendo en cuenta que, la rapidez con la que hoy en día se transmite la información a través de los medios tecnológicos es la misma con la que pueden perpetrarse los delitos.

Por lo que el objetivo planteado en esta investigación se relaciona a un estudio jurídico que permita demostrar La Vulnerabilidad Jurídica en Materia Penal Informática y su Escasa

Regulación dentro del Marco Legal Venezolano, el cual será estructurado para su realización en cuatro (04) capítulos que desarrollaran el problema:

Capítulo I: Describe el Planteamiento del Problema, las interrogantes de los investigadores, las cuales han sido convertidas en acciones investigativas, donde son base para el desarrollo del objetivo general, específicos y finaliza con la justificación, alcances y límites de la investigación.

Capítulo II: Desarrolla el Marco Teórico, describiéndose los antecedentes de investigación que guardan relación con el trabajo en estudio, presentando las teorías que permiten el entendimiento de la propuesta de solución, así como la fundamentación legal base para la investigación y, por último, la definición de términos que otorgan una mejor comprensión del tema en cuestión.

Capítulo III: Conformado por el Marco Metodológico, en el que se define el tipo de investigación, el diseño de investigación, las fases metodológicas, y las técnicas utilizadas para la recolección de datos; y por último,

Capítulo IV: Dirigido a los Resultados de la Investigación, donde el investigador debe abocarse a interpretar y analizar los resultados, para posteriormente conseguir conclusiones y así aportar recomendaciones que servirán de guía para futuros trabajos de investigación.

CAPITULO I

EL PROBLEMA

1.1 Planteamiento del problema

El avance de la sociedad es inevitable, desde que se crearon las señales de humo para emitir mensajes de auxilio el ser humano ha evolucionado hasta el punto de realizar video llamadas desde un continente a otro de manera inmediata a través de dispositivos electrónicos que caben en la palma de la mano. La tecnología evoluciona constantemente, cada vez más rápido, esto es productivo, pero también es perjudicial, pues así como progresa el ser humano y sus formas de realizar tareas cotidianas, también el avance tecnológico da lugar a la adopción de nuevas técnicas como instrumentos para producir resultados especialmente lesivos, lo que posibilita el surgimiento de nuevas modalidades delictivas.

La informática esta hoy presente en casi todos los campos de la vida moderna, se dice incluso, que la informática es una forma de Poder Social. El increíble desarrollo de la tecnología ha abierto las puertas a nuevas posibilidades de delitos antes inimaginables, como la manipulación fraudulenta de los ordenadores con ánimos de lucro, la destrucción de programas o datos y, el acceso y la utilización indebida de la información, lo cual afecta la esfera de la privacidad.

La ciberdelincuencia es un fenómeno conocido por la comisión de acciones perjudiciales perpetradas a través de medios tecnológicos con el fin de atacar redes, sistemas y datos. En términos generales se podría distinguir de los otros delitos ya que no tiene barrera físicas o geográficas, y se puede cometer con más facilidad y rapidez que los delitos comunes, entonces, la ciberdelincuencia es, todo delito que se pueda cometer usando computadoras, redes

computarizadas u otras formas de tecnología, sin embargo, ¿Cómo se sanciona a un individuo que haya cometido una acción perjudicial, si tales hechos no se encuentran tipificados como delito?

Con la pandemia del COVID-19, el aumento del nivel de los delitos relacionados con los sistemas informáticos representa una amenaza para las personas y por supuesto, para el ordenamiento jurídico, pues, luego de un año del confinamiento, nuevas formas de delinquir se han apoderado del internet, generando inquietud e inseguridad en la sociedad, y en algunos casos se está en presencia de especialistas que son capaces de borrar toda huella de los hechos, por esto es necesario tener un marco legal que este actualizado y acorde a conductas negativas dignas de ser tipificadas, porque de lo contrario, se da pie a la comisión de actividades tan actuales que no podrán ser sancionados debido a que no se tiene conocimiento siquiera de su existencia.

Ahora bien, en Venezuela, existe una escasa regulación con respecto a los delitos informanticos, claro que, es innegable que el legislador que elaboró la Ley Especial de Delitos Informanticos en el 2001 no podía prever los avances tecnológicos que ocurrirían en las siguientes dos décadas, ni el impacto que los mismos tendrían en el sistema jurídico Venezolano.

En consiguiente, la legislación sobre los delitos informanticos debe perseguir la protección integral de los sistemas que utilicen tecnología de información, y debe ser una Ley completa que regule el control, mitigación y prevención de los delitos informáticos. Por último, es necesario mencionar que, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

1.2 Formulación del problema

El bien jurídico tutelado en los delitos informáticos es, precisamente, la información en todos sus aspectos, es de hacer mención que no solo el Derecho, el Estado y los organismos internacionales tienen el deber de salvaguardarla, pues se trata de un trabajo en conjunto con el sector privado, la sociedad civil y por supuesto, la academia. En Venezuela los delitos cometidos a través de internet están a la orden del día, lo que nos lleva a plantearnos una serie de preguntas, a las cuales se les dará respuesta con el desarrollo y resultado de la presente investigación, siendo estas las siguientes interrogantes:

¿Cómo se le atribuye la cualidad de delito a las acciones perjudiciales que no están tipificadas en la respectiva Ley Especial?

¿Es eficaz la regulación que se usa para el control, mitigación y la prevención de la ciberdelincuencia en Venezuela?

¿Ha evolucionado el Derecho Penal informático en las últimas dos décadas en Venezuela?

¿El internet es una amenaza potencial para el derecho penal informático?

1.3 Objetivos de la investigación

1.3.1 Objetivo General

Demostrar la escasa regulación de la Ciberdelincuencia dentro del marco legal Venezolano.

1.3.2 Objetivos Específicos

1. Analizar La Ley Especial contra Delitos informáticos de Venezuela.

2. Determinar el avance que ha tenido el Derecho Penal Informático en las últimas dos décadas en Venezuela.
3. Identificar el impacto del internet en el Derecho Penal Informático Venezolano.

1.4 Justificación e Importancia del Estudio

La información que se posee actualmente no es la misma que dos décadas atrás, tampoco su forma de obtenerla o de archivarla, en consiguiente, los delitos que se perpetran en relación a ella, han evolucionado. Teniendo en cuenta que, la rapidez con la que hoy en día se transmite la información a través de los medios tecnológicos es la misma con la que se perpetran los delitos referentes al tráfico, violación o divulgación de la misma, la información tendrá la importancia que los poseedores le otorguen, y en la mayoría de los casos la sociedad no se percata de las grandes connotaciones que conllevaría su mal uso, partiendo de la premisa de que la información puede ser desde una clave de acceso hasta archivos con secretos de Estado.

Ahora bien, los delitos informáticos son aquellas acciones u omisiones que con el ánimo de perjudicar a otro o para favorecerse causando un daño a otro son realizadas a través de medios informáticos y que son penados por la Ley. En Venezuela, son penados a través de la Ley Especial contra Delitos Informáticos, la cual fue publicada en gaceta oficial N° 37.313, en fecha 30 de Octubre de 2001, sin embargo, en su artículo 32, se estableció una Vacatio Legis de treinta días, por lo tanto entró en vigencia oficialmente el día 30 de Noviembre de 2001, instrumento legal que contiene tan solo 33 artículos, y que desde su entrada en vigencia a la actualidad han pasado dos décadas, lo que la convierte en un tema de gran relevancia, pues la sociedad evoluciona cada día, y con ella las nuevas formas de perpetrar delitos por lo que el Derecho debe ir a su par, en consiguiente cuando se generan nuevas conductas o actividades perjudiciales

tienen que tipificarse para que se constituyan en delitos, en beneficio del control, mitigación y la prevención de la ciberdelincuencia en Venezuela.

Por otro lado, la actividad informática posee un gran potencial como medio de investigación, especialmente, debido a la ausencia de elementos probatorios que permitan la detección de los delitos que se cometan a través del uso de los ordenadores.

La realidad es que a la información en el país no se le ha dado el valor que merece, y en consiguiente, su resguardo carece de protección y seguridad, pudiendo ser un blanco fácil para ser viciada por cualquier persona o ente, por lo que es conveniente que se realice un estudio y análisis exhaustivo de la Ley Especial contra los Delitos Informáticos en Venezuela, se establezca el impacto que el internet tiene en el Derecho Penal Informático y por supuesto, se determine cuál ha sido su avance en las últimas dos décadas, todo con el norte de demostrar la escasa regulación que existe sobre los Delitos Informáticos dentro del Marco Legal Venezolano.

1.5 Alcances y Limitaciones del Estudio

Los alcances del Estudio, constituyen todo aquello que se espera de la investigación, es decir, los aspectos que se pretende alcanzar, siendo estos:

1. El presente estudio analizará la Ley Especial contra Delitos Informáticos.
2. La investigación abarcará únicamente lo relacionado a la Ciberdelincuencia y su regulación dentro del Ordenamiento Jurídico Venezolano.
3. Contribuir con la academia a reforzar los conocimientos y estudio acerca de los Delitos informanticos, su perpetración y sanciones. Siendo los beneficiados los estudiantes y futuros abogados que decidan especializarse por la materia penal.

4. Se analizan los riesgos que genera la escasa regulación que existe en materia informática dentro del Marco Legal Venezolano.

Durante el proceso de la investigación, se presentan ciertas limitaciones que dificultan de cierta forma el desarrollo eficaz de la exploración del tema, siendo estas:

1. La falta de información específica por ser un tema sumamente innovador.
2. Los cortes no programados de la energía eléctrica existentes en el país.
3. La constante falla del servicio de telecomunicaciones presente en Venezuela.

CAPITULO II

MARCO TEÓRICO

2.1 Antecedentes de la Investigación

Según, Ariza Diego (2017) en su tesis titulada; **Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso**, presentada como requisito para optar al grado de Maestro en Informática en la Universidad Pedagógica y Tecnológica, Sogamoso, Colombia, hace referencia a que el: *"progreso tecnológico puede ser portador de beneficios o de perjuicios, según como se encauce la voluntad humana, dando origen a nuevas situaciones que han provocado la necesidad de nuevas elecciones y decisiones"*, por lo tanto, las conductas irresponsables con respecto al mal uso de la información ha derivado en la clara evidencia de los profundos problemas y consecuencias en la que los jóvenes inexpertos o personas inescrupulosas incurren día a día, partiendo de esto tanto la legislación y el marco jurídico en general de la mayoría de los países han reconocido la importancia de defender los derechos con respecto a la información como valor esencial y a la protección de la misma, teniendo presente la vulnerabilidad adquirida con respecto a la incursión de distintas conductas negativas que puedan afectar a dicho elemento.

Por lo tanto el referido estudio guarda una estrecha relación con la presente investigación debido a que se denota lo importante que es el usuario y su intención para constituir una acción negativa en sí, empleando los medios tecnológicos para tal fin, lo relevante está en que tales medios pueden parecer ser inofensivos, pero la realidad es que pueden ser tan perjudiciales como útiles si tal como se menciona anteriormente la voluntad humana decida.

Por otra parte, Haarscher Agustina (2016) en su Trabajo de Grado titulado; **"Delitos Informáticos",** presentado como requisito para optar al título de abogado en la Universidad Empresarial Siglo XXI, Córdoba, Argentina, considera que el término delito Informático consiste en: *"la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando en elemento informático o telemático contra los derechos y libertades de los ciudadanos"*, lo que a su vez nos lleva a analizar el hecho de que si en efecto se trata de una conducta negativa que afecta los bienes jurídicos protegidos por el Estado no se les puede denominar delito a muchos debido a su falta de tipicidad en la norma penal, a pesar de que algunos solo se diferencien en el aspecto del medio para su comisión.

Por lo tanto queda en evidencia cierta vulnerabilidad con respecto a este tema, debido a que según la teoría general del delito, el mismo consta de ciertos elementos que le atribuyen esa cualidad, donde la descripción de la acción en la ley provee al marco jurídico de los denominados tipos penales.

Por otra parte, Acosta Eduardo (2012) en su trabajo de grado titulado "**Los delitos informáticos y su perjuicio en la sociedad"** presentado como requisito para optar al título de abogado en la Universidad Técnica de Cotopaxi, Latacunga, Ecuador, determina que: *"los delitos informáticos han sido poco estudiados y conocidos, en la actualidad a un no se ha logrado encontrar la fórmula para que todos estos sean sancionados, ya que no existen los medios necesarios para la persecución del este nuevo modo para infringir la ley, es así que el Estado debe garantizar los derechos de sus habitantes, creando los medios suficientes y necesarios para que estos no queden en la impunidad"*. Por lo tanto resulta pertinente traer a colación esta idea debido a que en consecuencia a este precepto ocurre un fenómeno bastante típico en la actualidad dentro del Marco Jurídico Venezolano y es la necesidad de encuadrar

forzosamente todas las acciones negativas en perjuicio de la sociedad cometidas a través de medios informáticos en la normativa vigente que debido a la fecha de su promulgación quedó obsoleta con el transcurrir del tiempo, entonces se busca adecuar cada acción en los tipos penales disponibles cuando los mismos guardan poca o ninguna relación, desproveyendo al mismo sistema de justicia de confiabilidad ya que dichos procedimientos están inmersos en distintos tecnicismos, que desde un principio se buscó castigar las acciones sin haberlas respaldado completa y anteriormente en una ley formal.

En consiguiente, Carrasquero Julio (2016) en su trabajo de grado presentado como requisito para optar al título de Abogado en la Universidad Dr. Rafael Belloso Chacín, Maracaibo, Venezuela, nos indica que es menester e importante la creación de: *"instrumentos jurídicos de tipo penal a la materia de participación y momento de ejecución de los hechos ciliados teniendo presente las diversas modalidades en las que se pueden suscitar los delitos informáticos para que sus actores ya no pasen desapercibidos ante la ley"* Por lo tanto es de hacerse notar que precisamente es fundamental el desarrollo del marco jurídico venezolano en lo que a derecho penal informático respecta debido a que existen tantas modalidades en las que se pueden perpetras dichas acciones perjudiciales que de no hacerlo puede causar gravámenes irreparables, debido a que por cierto, dichas modalidades incrementan con el transcurrir del tiempo, tal cual lo hace la tecnología.

Por último, se considera importante traer a colación lo que nos indica Uzcategui Amaury (2007) en su tesis titulada **"El comercio Electrónico, los Delitos Informáticos y su Legislación en Venezuela"** presentada como requisito para optar al título de Magister Scientiae en Administración en la Universidad de los Andes, Mérida, Venezuela, por lo tanto se aprecia que: *"En la sociedad de la información actual todos los ámbitos del quehacer humano se ven*

acomedidos, manejados o afectados por el hecho tecnológico. Las aplicaciones de la ciencia invaden las actividades humanas sin que prácticamente nada escape a ello: las nuevas fuentes de energía, la automatización y la organización científica de la agricultura y las manufacturas, los transportes, la conquista espacial, la salud, las costumbres… Esto genera una suerte de dependencia hacia la tecnología, la cual se observa con claridad en la industria, la banca, en casi toda actividad pública como los sistemas tributarios, electorales y en el comercio" Por lo tanto una vez más queda demostrado que tanto está involucrada la tecnología en la vida cotidiana, al tener eso como una proposición queda establecido que cada día el ser humano y la sociedad en general se vuelve más dependiente de la tecnología a una escala inimaginable, donde incluso prevalecen más las relaciones digitales que las físicas, por lo tanto resulta de una importancia inconmensurable que el Estado busque proteger y resguardar el desenvolvimiento de la sociedad en lo que al Derecho Penal Informático se refiere, pues prácticamente la vida está migrando a la tecnología.

2.2 Bases Teóricas

La principal fuente es la teoría, e indudablemente es la que facilita el entendimiento de los conceptos, que de una manera directa desarrollan el tema propuesto. En la presente sección de la investigación se desglosa la perspectiva teórica, proporcionando una visión sobre donde se sitúa el planteamiento propuesto dentro del campo de conocimiento del estudio, analizando la estructura de los sistemas bibliotecológico de clasificación y encontrando que tipo de relación existe entre los elementos.

En consiguiente, las bases teóricas, ayudan al investigador a tener una visión clara o un enfoque lógico, que permita explicar detalladamente la investigación planteada, por lo tanto, se

implementan las bases de la variable de conceptos que poseen conexión con la investigación actual, combinando opciones antes de mejorar las teorías.

Ahora bien, la raza humana tiene alrededor de siete millones de años de evolución, que no existiría de no ser por la transmisión de información evolutiva pasada de generación en generación, así pues, la esencia de la raza humana es la información, bien sea genética o de carácter social, la información tiene tanta importancia como la que los poseedores le otorguen y es tan sobrevalorada que en la mayoría de los casos la sociedad no se percata de las grandes connotaciones que conllevaría su mal uso, partiendo de la premisa en la que la información puede ser una clave de acceso, hasta archivos con secretos de estado.

En pleno siglo XXI se ha normalizado obtener la información de manera fácil, económica y directa a través del internet y las plataformas digitales, su transmisión a otras personas se ha vuelto una acción casi inmediata, rompiendo las fronteras y pudiendo esparcirse una noticia alrededor del mundo en cuestión de horas, sea de cualquier índole o interés, pudiendo así alterar su percepción o tergiversándola e incluso, comerciando con esta.

Sin embargo, la realidad es que a la información en Venezuela no se le ha dado la importancia que esta amerita, por lo tanto su resguardo carece de protección y seguridad, pudiendo verse viciada por cualquier ente o persona y su marco legal tiene una desactualización de más de 20 años siendo esto una vulnerabilidad inminente que perjudica tanto al Estado como a los particulares, a diferencia de otros países con un desarrollo más prominente en donde todas las acciones referentes a la manipulación de información están fuertemente reguladas y supervisadas así como sancionadas, lo que impide que esta sea vulnerable ante cualquiera que no corresponda su uso, según el tipo de información que se trate. En el mismo orden de ideas, se

describirán a continuación aquellos conceptos relacionados con el estudio jurídico en cuanto a la Vulnerabilidad Jurídica en materia penal informática.

Derecho Informático

El Derecho Informático se define como el área del Derecho que regula los efectos jurídicos derivados de la informática y demás aspectos tecnológicos de igual manera que las denominadas Tecnologías de Información y Comunicación (TIC), en este aspecto se puede apreciar que el Derecho Informático abarca una amplitud de competencias que van desde los Delitos Informáticos hasta las Relaciones Laborales que pueden establecerse a través de los medios informáticos, de la misma manera aplica en los casos de propiedad intelectual e incluso la contratación informática.

Según Hernández Díaz (2009), la delincuencia informática se encuadra dentro de lo que se conoce como "Derecho informático" lo cual define como el conjunto de normas jurídicas que regulan la utilización de los bienes y servicios informáticos en la sociedad incluyendo como objeto de estudio: 1º el régimen jurídico del software; 2º el derecho de las Redes de transmisión de datos; 3º los documentos electrónicos; 4º los contratos electrónicos; 5º el régimen jurídico de las bases de datos; 6º el derecho de la privacidad; 7º los delitos informáticos; y 8º otras conductas nacidas del uso de los ordenadores y de las redes de transmisión de datos.

Ciberdelincuencia

Agencia de la Unión Europea para la Cooperación Policial Europol (2018) distingue la ciberdelincuencia en delitos "*dependientes de los medios informáticos*" es decir, "todo delito que solo se puede cometer usando computadoras, redes computarizadas u otras formas de tecnologías de la información y comunicación". De la misma forma, a saber no existe una

definición universalmente aceptada en lo que respecta a la Ciberdelincuencia, A pesar de esto hay concordancia en los distintos aspectos o elementos que deben concurrir para que se pueda llegar a determinar un ciberdelito estos son comunes a las distintas definiciones que se le ha atribuido a la referida figura.

Por lo tanto se puede determinar que para poder identificar un ciberdelito es necesario poder apreciar que a priori el acto ejecutado infrinja la ley o en caso contrario produzca un gravamen a particulares, el Estado o la sociedad y este debe ejecutarse o cometerse empleando las Técnicas de Información y Comunicación (TIC) o en lo que respecta, cualquier dispositivo electrónico, empleando su uso para atacar redes, sistemas, datos o sitios web. En este aspecto, se puede definir que los ciberdelitos en su mayoría empleados por piratas cibernéticos o hackers afectan de forma negativa la confidencialidad, integridad o accesibilidad de los sistemas y datos informáticos a través del empleo de distintos algoritmos codificados para causar perjuicios, tales como: Troyanos, Gusanos Informáticos y bombas lógicas.

Vulnerabilidad Jurídica

La Real Academia Española define como vulnerable (del latin vulnerabilis) a quien *"puede ser herido o recibir lesión, física o moralmente"* De tal manera que cuando se esté al frente de una situación en donde se pueda sufrir algún daño se trata de vulnerabilidad, la cual representa un estado de debilidad provocada por la ruptura del equilibrio que conlleva a un espiral de efectos negativos.

Cuando se hace referencia a la vulnerabilidad jurídica se trata de esa fragilidad legal o jurídica que posee determinado aspecto en el ámbito del Derecho, pudiendo adecuarse a una norma o a algún precepto legal, que en el caso de estar bajo esta situación, existe la probabilidad

de que ocurran determinados acontecimientos no previsibles que puedan generar consecuencias negativas significativas sobre ciertos aspectos en el Derecho aumentando incluso su peligrosidad, en virtud de la magnitud, duración, frecuencia e historia, lo que condiciona per se el estado de la vulnerabilidad.

Entre las causas que colocan al Marco Jurídico de un Estado en situación de vulnerabilidad está el desamparo ocasionado por no contar con los instrumentos legales correspondientes para resguardar los bienes jurídicos tutelados por el Estado, o en caso de que se cuenten con estos, los mimos incurren en lagunas legales, vacías legales, tecnicismos jurídicos y su desactualización conforme transcurre el tiempo, debido a que tal como la sociedad evoluciona, lo debe de hacer el Derecho, que es la ciencia que puede llegar a regular su conducta, en caso contrario, pues la vulnerabilidad se verá al acecho.

2.3 Bases Legales

Dentro la legislación venezolana encontramos varias regulaciones que tipifican los delitos correspondientes al tráfico, violación y la divulgación de la información, así mismo podremos apreciar el vacío que existe a causa de la desactualización y la vulnerabilidad jurídica que posee nuestra legislación en materia de penal informática debido a este vacío, estas serán citadas en orden de supremacía según su peso dentro del derecho venezolano.

Nuestra Carta Magna publicada en G.O. N° 36.860 de fecha 30 de diciembre de 1999, establece en su artículo 48 un precepto constitucional que resulta pertinente citar debido a la relación que guarda con el tema, este establece que *"Se garantiza el secreto e 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 el artículo citado podemos apreciar distintas cosas, entre ellas, el objeto jurídico que se buscaba resguardar, que no es más que la inviolabilidad de las comunicaciones privadas, respetando así la privacidad y el derecho de expresión, pero también encontramos una pequeña falla, y es el año en que esta norma fue emitida, finales del año 1999, para ese entonces se hacía referencia a las comunicaciones por vía telefónica y era imposible prevenir que un año más tarde saldría a luz pública y comercial el uso del ordenador y con este los medios digitales, mutando los delitos de violación de privacidad e información a unos medios más convencionales para los cuales los cuerpos de seguridad no estarían preparados.

En el Código Penal venezolano, en su libro segundo, capítulo V, artículos 185, 186, 187, 188, 189 y 190 se encuentra establecida la inviolabilidad del secreto, en ese pequeño compendio de artículos el legislador tipifica acciones como *"el que indebidamente abra una carta, telegrama o pliego cerrado que no se le haya dirigido"*, *"cualquiera que haya suprimido indebidamente alguna correspondencia epistolar o telegráfica que no le pertenezca"* también *"el que la hiciere indebidamente publica"* tendrá una sanción, de igual manera el que haciendo uso de su privilegio por *"sus funciones, estado, profesión, arte u oficio"* realice las acciones antes mencionadas será castigado con arresto, prisión o multa según la acción que haya cometido.

Nuevamente podemos apreciar la falta de actualidad que posee nuestra legislación refiriéndose a *"cartas, telegramas o pliegos"*, cuando la realidad es que los delitos que violan la privacidad y la información son perpetrados de otras maneras y por otros medios ya que las

personas no hacen uso de los medios antes mencionados debido a su descontinuación en el uso cotidiano, y por lo tanto los delincuentes no los atacan.

Por otra parte tenemos la Ley Especial contra los Delitos Informáticos, esta fue promulgada en el 2001 y se compone de treinta y tres artículos comprendidos en cuatro títulos los cuales tienen por objeto "*la protección integran 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".*

Esta norma contempla con una mayor cobertura los delitos relacionados al tráfico de información sin embargo, a pesar de que esta ley busca abordar el problema de una manera directa, carece de actualidad debido a que fue promulgada en el 2001 y en la actualidad, 20 años más tarde, la tecnología ha avanzado a escalas incalculables, sumiendo al Estado en una vulnerabilidad jurídica que es pertinente abordar antes de que las consecuencias sean irreparables.

Para dirigirnos hacia el caso concreto es necesario partir del título II de esta norma, en donde apreciamos que se el legislador tipifica los delitos relacionados con la materia, estos los separa en cuatro capítulos divididos según a donde se perpetre el delito, estos son:

- Contra sistemas informáticos que utilizan tecnologías de información
- Contra la propiedad
- Contra la privacidad de las personas y las comunicaciones
- Contra el orden público

Entre los artículos pertenecientes a los mencionados capítulos, se encontraron varios fallos como, términos y conceptos anticuados, en desuso y desactualizados, debido a que los términos

que se emplean ya mutaron y tienen diversas denominaciones así como diversas variaciones y modificaciones que permiten otra interpretación a la norma y así mismo permiten al delito refugiarse en tecnicismos jurídicos quedando impunes las acciones ya que carecen de una tipicidad expresa en la norma, y si bien se pudiese encuadrar las acciones en determinados tipos, estos carecen de actualización y por lo tanto la sanción sería una nimiedad comparado con el daño que produciría el delito.

Como es el caso en el artículo 2 en donde el legislador denomina "tecnología de información" a una rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, atrasándose a los delitos perpetrados a través de los medios digitales y la conexión a internet, que es por donde actualmente ocurren el 90% de los delitos informáticos, esto conlleva a que los delitos previstos en el título II, capítulo I, posean un vacío de forma.

En el mismo artículo encontramos otra denominación la cual es "tarjeta inteligente", aquí el legislador lo define como *"rótulo, cédula o carnet que se utiliza como instrumento de identificación, de acceso a un sistema, de pago o de crédito y que contiene data, información o ambas"* ahora, el legislador aplica esta definición para referirse más que todo a la clonación de tarjetas de débito y crédito y a identificaciones que posean chips que permitan el acceso a los sistemas, pero en la definición no aparece la palabra "chip", pudiéndose nuevamente interpretar de distinta manera a falta de exactitud en la norma, ya que una cedula y un carnet es un documento de identificación, contiene data e información, pero no necesariamente posee un chip.

La norma también ignora el alcance remoto de estos delitos a través del internet, tomando en cuenta solo el acceso físico a los denominados sistemas que usan "tecnología de información" como el sabotaje informáticos, además, la norma tipifica la comisión de acciones ya tipificadas

con la única diferencia de su modo de comisión y no previene los nuevos delitos que se perpetran en la actualidad, como es el caso del artículo 12, 13 y 14 en donde se re tipifica la falsificación de documentos, el hurto y el fraude.

Esto lo podemos apreciar en los delitos referentes a la privacidad de las personas y de las comunicaciones, los cuales poseen poco alcance debido a que, nuevamente por la falta de actualidad en la ley, se pasa por alto que actualmente la mayoría de estos delitos se perpetran por redes con conexión a internet y no por "sistemas con tecnología de información", sino a través de redes sociales, este es un medio no previsto por la ley y si bien, se podría encuadrar dicho medio en algún tipo de esta norma, siempre se encontraran vacíos que nuevamente permiten al delito refugiarse en tecnicismos jurídicos.

Así, por ejemplo, el artículo 12 castiga al que "indebidamente" crea, modifica o elimina un documento o cualquiera de sus datos contenidos en un sistema informático o, de cualquier forma, incorpora en un sistema informático un documento ajeno a este. Si se efectúa una lectura profunda de este artículo se puede analizar que se podría castigar a cualquiera que traduce (modifica) un documento descargado de Internet o descarga un archivo de Internet desde la computadora de la oficina (incorpora en un sistema informático) por el delito de falsificación de documentos informáticos, ya que, la Ley es tan genérica que no queda claro qué conductas son las "debidas de realizar" en cada caso y no identifica claramente cuál es el agravio.

Por otra parte, se aprecia que en el artículo 27 se establece una agravante si para la comisión del hecho se hace uso de una contraseña obtenida indebidamente y en otro supuesto, si se comete mediante el abuso de posición por razón del ejercicio de un cargo o función, pero para efectos de la perpetración de los delitos mencionados con anterioridad, esas agravantes toman a

la ligera la situación ya que se determinó que para la perpetración de esos delitos se flagela la seguridad de una manera más violenta y astuta.

De manera tal, que en varios artículos se señala como delitos a ciertas conductas se llevan a cabo sin "autorización" o de forma "indebida", pero no señala quien debe proporcionar dicha autorización o bajo qué condiciones debe otorgarse. Lo que genera confusión entre los operadores jurídicos y en algunas ocasiones ser utilizada para inculpar a personas bajo criterios distintos de los que inspira la norma de una manera totalmente subjetiva, es aquí donde se hace necesario mencionar un viejo principio que rige las reglas de la interpretación como lo es *"donde no distingue el legislador no podrá hacerlo el intérprete"*.

A pesar de esto, poseemos una ley orgánica promulgada un año más tarde denominada "Ley Orgánica de Seguridad de la Nación", el cual es un compendio de normas establecidas para perseguir el orden y la seguridad del Estado y sus particulares, en dicho compendio se encuentran un artículo que es de particular interés para este informe, este es el artículo 14, que dicta los riesgos tecnológicos y científicos, establece que *"El Estado tiene la obligación de vigilar que las actividades tecnológicas y científicas que se realicen en el país no representen riesgo para la seguridad de la Nación*", ¿Cómo hacer esto si no se está actualizado en materia tecnológica?

Debido a la vulnerabilidad jurídica en la materia resulta imposible que el Estado pueda vigilar actividades tecnológicas y que estas no representen riesgo para la seguridad de la nación, cuando el Estado esta tan desactualizado en términos de tecnología, tanto que se escapa de su posibilidad el control de los delitos actuales referentes a la materia informática, materia que es parte de la tecnología actual. Por otro lado, se puede observar el gran potencial de la actividad

informática como investigación, especialmente debido a la ausencia de elementos probatorios que permitan la detección de los ilícitos que se cometan mediante el uso de los ordenadores.

2.4 Definición de Términos Básicos.

- **Sabotaje informático**: Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son: virus, gusanos, y bomba lógica o cronológica, los cuales se detallan a continuación.
- **Virus:** Es una serie de claves programáticas que pueden adherirse a los programas informáticos legítimos y propagarse a otros. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como mediante el método del caballo de Troya.
- **Gusanos:** Se fabrican de forma análoga al virus con miras a infiltrarlos en programas legitimas de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos, podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita
- **Bomba lógica o cronológica:** Exige conocimientos especializados ya que requiere programar la destrucción o modificación de datos en un futuro. Ahora bien, a diferencia de los virus o de los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos Informáticos criminales, son las que poseen el

máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente, La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar donde se halla.

- **Acceso no autorizado a sistemas o servicios Por motivos diversos:** desde la simple curiosidad, como en el caso de muchos piratas informáticos (hacker) hasta el sabotaje o espionaje informático.
- **Piratas informáticos o hackers:** El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación, El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para tener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder en aquellos sistemas en los que los usuarios pueden emplear contraseñas comunes o de mantenimiento que están en el sistema
- **Troyano:** Sistema algorítmico programado para invadir un sistema o dispositivo tecnológico con el fin de acceder a este de manera remota, con la particularidad de que dicho virus de acceso aparenta ser un documento de multimedia común y corriente con la finalidad de no levantar sospecha, su nombre deriva del popular “caballo de Troya” dándole sentido a su función.

CAPITULO III

MARCO METODOLÓGICO

3.1. Tipo de Investigación

El autor Arias F (2017) define la investigación documental como *"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"*. Ahora bien, como en toda investigación el propósito de esta es el aporte de nuevos conocimientos, la investigación jurídica documental propone estudiar el ordenamiento jurídico para conocerlo y aportar recomendaciones para mejorarlo.

En consiguiente, la presente investigación se enmarca dentro de una investigación documental. Este tipo de investigación requiere que el investigador dedique bastante tiempo a la revisión de textos, como las normas, la jurisprudencia, la doctrina, en general, material relevante y pertinente a su objeto de estudio, a través de los cuales identifica categorías de análisis, marcos teóricos y líneas jurisprudenciales, información que al ser recogida debe ser registrada y sistematizada para posibilitar su análisis e interpretación.

3.2. Diseño de Investigación

El Diseño de Investigación, es el planteamiento de una serie de actividades sucesivas y organizadas, que se adaptan a las particularidades de cada modalidad de investigación, y que indican los pasos y pruebas a efectuar, así como las técnicas para la recolección de los datos necesarios al objeto de estudio (Tamayo y Tamayo, 2003, p. 124).

En consiguiente, el diseño de investigación puede definirse como los métodos y técnicas elegidos por un investigador para combinarlos de una manera razonablemente lógica para que el

problema de la investigación sea manejado de manera eficiente y para cada uno existen diferentes técnicas de recolección de datos, por lo que resulta de gran importancia determinar cuál es el diseño de investigación adecuado para la presente investigación para luego usar los métodos de recolección de datos o información adecuados, ya que el primero influye en el segundo.

Así pues, el diseño de investigación de este trabajo es un diseño Bibliográfico, el cual se aplica cuando se usan datos secundarios, es decir, aquellos que han sido obtenidos por otros, y donde el investigador tiene como fin resolver el problema planteado, siguiendo el orden de las fases metodológicas, siendo estas:

Fase I: Analizar La Ley Especial contra Delitos informáticos de Venezuela.

Esta fase tiene como objetivo analizar la ley especial de la referida materia con el fin de lograr un entendimiento profundo acerca de las circunstancias que vuelven vulnerable nuestro marco jurídico, dotando nuestra norma de vacíos legales, lagunas legales y tecnicismos jurídicos, además se podrá evaluar si realmente la desactualización de la norma influye de manera negativa en el sistema jurídico, dado que el transcurrir del tiempo, vuelve los dispositivos legales obsoletos, por lo tanto se procederá a desentrañar los artículos del referido dispositivo legal especial con el fin de obtener un análisis completo del mismo.

Fase II: Determinar el avance que ha tenido el Derecho Penal Informático en las últimas dos décadas en Venezuela.

La presente fase tuvo como principio fundamental realizar un estudio profundo para así determinar cuánto ha sido el avance del Derecho Penal Informático en los últimos 20 años, con

el propósito de demostrar su escaso avance, esta fase constituye un aporte primordial para la presente investigación debido a que es fundamental el avance del tiempo ya que es el factor que agrava la vulnerabilidad jurídica en la materia e incrementa los perjuicios que puedan ser provocados por la informática y la tecnología, por lo tanto es fundamental que la relación entre estos dos aspectos sea lo más equitativa posible ya que si en efecto hay una disparidad notable, quedaría en evidencia lo vulnerable que puede ser la sociedad y el Estado en lo que al Derecho Penal Informático se refiere.

Para lograr la efectividad de ésta fase, se utilizaron técnicas documentales como la hemerografía sustentada en diferentes portales web, específicamente en el estudio y análisis de distintos instrumentos que permitieron ampliar la información disponible sobre el referido tema para un análisis general, para poder partir hacia conclusiones un poco más específicas.

Fase III: Identificar el impacto del internet en el Derecho Penal Informático Venezolano.

La fase tres estuvo fundamentada en el señalamiento de los efectos que se ha generado en la sociedad venezolana y como ha impactado de manera negativa en la sociedad, permitiendo la comisión de acciones perjudiciales y la innovación en lo que respecta a nuevas maneras de causar las mismas, las cuales no pueden denominarse delitos porque no se encuentran la mayoría tipificadas en alguna ley penal, es por eso que por medio de recopilación de información, se ha permitido observar la magnitud de la situación social en cuanto a la respuesta negativa de los mecanismos legales frente a las referidas situaciones.

3.3. Técnicas de Recolección de Datos

"...El procesamiento de los datos no es otra cosa que el registro de los datos obtenidos por los instrumentos empleados, mediante una técnica analítica en la cual se comprueba la hipótesis y se obtienen las conclusiones..." (Tamayo 2001 p.103)

La presente investigación se realizó mediante la técnica de revisión documental, en el que el investigador se fundamentó en la determinación de carácter de los documentos, desechando aquellos que no aportaron información pertinente al objeto de estudio con el fin de reducir la recolección a términos que coincidieran con el ámbito de la información. Así mismo, Chávez (2004) establece que la revisión documental *"constituye la sustentación teórica del estudio, a través de la interpretación de las distintas corrientes, doctrinas y enfoques especializados que existen respecto a la investigación"* (p. 63).

Así pues, por ser una investigación jurídica dogmática, se tomó en cuenta la Legislación, ya que el objetivo principal de la presente investigación es realizar Demostrar la escasa regulación de la Ciberdelincuencia dentro del marco legal venezolano, por lo que se dispuso de la Constitución de la República Bolivariana de Venezuela, El Código Penal Venezolano, la Ley Especial contra delitos informáticos y la Ley Orgánica de Seguridad de la Nación.

3.4. Fuentes de Conocimiento Jurídico

Las fuentes del conocimiento jurídico según Sánchez N (2005) son el "*conjunto de datos y actos que dan nacimiento a un orden normativo y sirven para analizar, evaluar, y comprender los fenómenos socio-jurídicos de un lugar determinado*".

Así pues, el investigador puede inclinarse a enfocar el problema jurídico desde una perspectiva legalista o dogmática por lo que el objeto a investigar será el material legal o legislativo, usando como fuentes jurídicas directa la Ley, siendo estas:

- Constitución de la República Bolivariana de Venezuela. Gaceta Oficial No. 36.860 (Extraordinario). Diciembre 30, 1999.
- Ley Especial Contra los delitos Informáticos. Gaceta Oficial No. 37.313. Octubre 30, 2001.
- Ley Orgánica de Seguridad de la Nación. Gaceta Oficial No. 37.594. Diciembre 18, 2002.
- Código Penal Venezolano. Gaceta Oficial No. 5.768 (Extraordinario) Abril 13, 2005.

CAPITULO IV

RESULTADOS DE LA INVESTIGACIÓN

4.1. Análisis e Interpretación de los Resultados

Desde el principio de los tiempos la humanidad o el hombre han ido creando una larga serie de normas tendientes a regular la convivencia en sociedad. Pero, mientras unos se dedican a elaborar la Ley, los otros se idean como evadirla o realizar la "trampa", así pues, para defenderse de quienes intentan burlar la ley, el Derecho, a través de sus operadores en los diferentes campos, fue delineando diferentes soluciones.

Ahora bien, a través de los sistemas informáticos, se pueden entregar datos e informaciones sobre miles de personas, naturales y jurídicas, en aspectos tan fundamentales para el normal desarrollo y funcionamiento de diversas actividades, ejemplo, actividades bancarias, financieras, tributarias, y de identificación de las personas.

En consiguiente, si a ello se agrega que existen entidades dedicadas a proporcionar, si se desea, cualquier información, sea de carácter personal o sobre bienes a los particulares; se comprenderá que la magnitud del asunto, pues todos esos datos están en juego o podrían ha llegar a estarlo, si no se les da el uso debido u autorizado, por lo que el ordenamiento jurídico debe ir un paso más adelante y proteger la información de la ciberdelincuencia, mediante una ley capaz de prevenir, mitigar y castigar estos actos lesivos que atenten contra los bienes jurídicos que deben ser tutelados por el Estado.

Fase I: Analizar La Ley Especial contra Delitos informáticos de Venezuela.

Los resultados obtenidos en esta fase no son más que los conocimientos jurídicos necesarios para poder determinar si en efecto la Ley actual es acorde a las situaciones que acontecen el día a día en lo que al Derecho Penal Informático se refiere, al haber efectuado un

profundo análisis de la Ley Especial contra Delitos Informáticos se ha podido determinar que a pesar de que para su promulgación, el referido instrumento fue bastante innovador y productivo, ahora debido al gran auge en lo que respecta a las acciones perjudiciales cometidas a través de medios electrónicos e informáticos la ley se encuentra en decadencia al incurrir en ciertos vacíos legales y lagunas jurídicas.

Otro factor importante es el de la generalidad de la norma especial, lo que ocurre cuando en ciertos tipos penales se busca encuadrar todo tipo de acción que se asemeje así sea en lo más mínimo, siempre que guarde relación con la informática, esto produce ciertos tecnicismos ya que uno de los principios que regulan la materia penal es "**nullum crimen, nulla poena sine lege**" por lo tanto no puede haber pena sin delito, y en consecuencia no puede haber delito si el mismo no está previsto en la ley, tal como lo establece el artículo 1° del Código Penal Venezolano *"Nadie podrá ser castigado por un hecho que no estuviere expresamente previsto como punible por la ley, ni con penas que ella no hubiere establecido previamente"*

Por otra parte algunas de las definiciones contenidas dentro de la norma presentan errores o están incompletas en lo que a términos de definición se refiere, además de ello también deberían de incluirse una mayor cantidad de términos para que de esa manera se pueda garantizar y contemplar acciones sobre otros medios informáticos bajo los cuales se perpetran delitos tipificados en dicha norma.

Fase II: Determinar el avance que ha tenido el Derecho Penal Informático en las últimas dos décadas en Venezuela.

En lo que respecta al avance dentro del Derecho Penal Informático, el mismo es deplorable, debido a que la tecnología avanza a tal escala que las innovaciones en el año 2000 se duplicaron en el año 2001, las del año 2002 duplicaron las dos anteriores, y así sucesivamente a

tal punto de que los avances contenidos en el transcurso del año 2020 y 2021 son increíblemente superiores a los que ha habido desde el año 2000 hasta el 2019, por lo tanto, al tener en cuenta esto, resulta evidente que si la referida Ley Especial es del año 2001 y se ocupó de abarcar las figuras anteriores a ese año, como se puede esperar que el mismo dispositivo puedan mantenerse acorde a las figuras delictivas si tenemos en cuenta el criterio en el que la tecnología duplica sus avances con cada año que transcurre, el hecho de que se logre imputar a los sujetos que incurran en distintos supuestos que se puedan asemejar a los dispuestos en la norma no significa que le norma se mantiene, más bien la fuerzan a mantenerse y no es el hecho, el Derecho Penal debe ser exacto e inequívoco por lo tanto no se puede pretender tipificar una acción general cuando la comisión de la misma exige que se determinen distintos supuestos en donde se pueda aplicar una pena acorde a la comisión de los mismos.

Fase III: Identificar el impacto del internet en el Derecho Penal Informático Venezolano.

Gracias a los avances tecnológicos de los últimos años, la manera de acceder a internet resulta mucho más fácil y económica que en las últimas décadas, por lo tanto de igual manera resulta más fácil perpetrar acciones perjudiciales o delitos informáticos ya que prácticamente el medio más importante de comisión es el internet y el acceso a este no es muy limitado, partiendo de la premisa en la que actualmente es más fácil acceder a internet que tener acceso a un arma, mucho más económico, más discreto y al alcance de todos sin distinciones económicas.

Por tanto esto, tan solo basta con realizar una contraposición entre lo que se puede hacer con internet y lo que regula nuestro marco jurídico, de la misma manera observar si los entes y organismos pertinentes pueden actuar o abarcar las situaciones que puedan generarse por el mal uso del internet. Si se tiene en cuenta los grandes avances que se han observado en la tecnología

en los últimos años, podemos percatarnos de que mucho no hubiese podido ser posible sin el uso del internet, por lo se puede apreciar el gran poder que dicha herramienta tiene, es por esto que es alarmante el hecho de que si nuestro marco jurídico no está a la altura de los avances tecnológicos, ¿cómo puede estarlo a la del internet? Si el mismo es el que precisamente ha permitido los avances del fenómeno que volvió vulnerable a toda una sociedad dejándola a la intemperie en lo que a Delitos Informáticos se refiere.

4.2. Conclusiones

Actualmente, en casi todos los país se ha digitalizado la información, tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en el estudio y, evidentemente, en el ocio. El uso de la informática es en ocasiones indispensable y hasta conveniente. No obstante, junto a las indiscutibles ventajas que presenta, comienzan a surgir algunas desventajas o aspectos negativos, por ejemplo, lo que ya se conoce como "Ciberdelincuencia". Así pues, al llegar a este punto se debe notar que cada cierta década el Derecho Penal se ve superado por la realidad, realidad que indica su desactualización como protector social y la necesidad de una reforma.

En el mismo orden de ideas, se sabe que la humanidad no está frente al peligro de la informática, sino frente a la posibilidad de que individuos o grupos de delincuencia organizada, con aspiraciones de obtener el poder que la información puede conferirles, la utilicen para satisfacer sus propios intereses, a costo de las libertades individuales y en contra de las personas.

Así mismo, puede afirmarse que hoy las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso, por lo que la amenaza futura será directamente proporcional a los adelantos de las tecnologías

informáticas. Es necesario tomar en cuenta que cuando se publica la información en Internet deja de ser privada y puede caer en manos de un ciberdelincuente. Por lo que a través de la presente investigación se llega a concluir lo siguiente:

- Dentro del marco legal Venezolano existe una escasa regulación sobre la Ciberdelincuencia, pues al analizar el ordenamiento jurídico, y en especial La Ley Especial contra Delitos informáticos de Venezuela, el investigador se pudo percatar que en efecto la referida incurre en vacíos legales, lagunas jurídicas y tecnicismos que no permiten una correcta aplicación de la misma.
- El avance que ha tenido el Derecho Penal Informático en las últimas dos décadas en Venezuela, es sorprendentemente deplorable, puesto que en 20 años la tecnología ha avanzado hasta el punto de crear un mundo alterno basado en la realidad virtual digno de una novela de ficción, y en esos mismos 20 años la ley especial no ha tenido ni una reforma.
- Como consecuencia del punto anterior es evidente el gran impacto del internet en el Derecho Penal Informático Venezolano, puesto a que si no se está actualizado con las tecnologías novedosas, tampoco se estará con lo que dicha tecnología es capaz de hacer mediante el uso de internet.
- Por otra parte, no es la amenaza potencial de la computadora o equipos electrónicos sobre el individuo lo que provoca desvelo, sino el uso que el hombre le dé, es decir, la utilización real por el hombre de los sistemas de informaciones con fines perjudiciales que atenten sobre los bienes jurídicos tutelados por el Estado.

- No son los grandes sistemas de información los que afectan la vida privada sino la manipulación por parte de individuos poco conscientes e irresponsables de los datos que dichos sistemas contienen.

4.3. Recomendaciones

- Que se determine en la Ley, en cada caso, cuando se entenderá que existe una autorización para el uso o aprovechamiento debido de un sistema informantico, así como la manera en la que esta será aprobada u otorgada.
- Que se determine cuando es un uso "indebido" de los sistemas informáticos.
- La legislación sobre protección de los sistemas informanticos debe perseguir acercarse lo más posible a establecer tipos penales que puedan adecuarse correctamente a las innovaciones delictivas con respecto a la materia.
- A la Universidad José Antonio Páez, incluir dentro del plan de estudio de la catedra de Derecho Penal, o como catedra nueva, temas relativos al Derecho Penal informantico, o al Derecho Informático como tal, pues como se planteó anteriormente es también trabajo de la academia formar mejores profesionales en el área, partiendo desde el punto que la tecnología evoluciona cada día y con ella debe evolucionar el derecho y la sociedad.
- A la sociedad, cuidar lo que se publica en Internet, en redes sociales, y de qué manera protege su información, pues todo lo que se hace en la red puede caer en manos de un ciberdelincuente. Es necesario evitar ingresar en enlaces sospechosos, pues pueden ser un intento de fraude cibernético. Desconfiar de cualquier enlace o dirección web no reconocida o no oficial, sobre todo si son enviados por correo electrónico o aparecen en ventanas emergentes mientras se navega por la web.

REFERENCIAS

Fuentes Bibliográficas

- Agencia de la Unión Europea para la Cooperación Policial (2018) *Informe sobre la Ciberdelincuencia,* pág. 15.
- Chávez (2004) Proceso Metodológico en la Investigación (Cómo hacer un diseño de investigación). Ediluz. Maracaibo, Venezuela. Pág. 63
- Hernández D. (2009) *El delito informático.* San Sebastián, Perú. Pág. 23
- Tamayo y Tamayo (2003). *El Proceso de Investigación Científica*. Limusa, México.

Fuentes Web

- Real Academia Española. "Vulnerable" Extraído el 25 de Noviembre de 2021 desde https://dle.rae.es/vulnerable
- Sánchez, N. (2005) "Fuentes del Conocimiento Jurídico" Extraído el 29 de Noviembre de 2021 desde https://www.monografias.com/docs/Fuentes-Del-Conocimiento-Jur%C3%ADdico-P349C5VFJ8U2Z

Fuentes Normativas

- Constitución de la República Bolivariana de Venezuela. Gaceta Oficial No. 36.860 (Extraordinario). Diciembre 30, 1999.

- Ley Especial Contra los delitos Informáticos. Gaceta Oficial No. 37.313. Octubre 30, 2001.

- Ley Orgánica de Seguridad de la Nación. Gaceta Oficial No. 37.594. Diciembre 18, 2002.

- Código Penal Venezolano. Gaceta Oficial No. 5.768 (Extraordinario) Abril 13, 2005.

Fuentes Trabajo de Grado

- Acosta, E. (2012) **"Los delitos informáticos y su perjuicio en la sociedad".** Universidad Técnica de Cotopaxi, Latacunga, Ecuador.
- Carrasquero J. (2016) **"Derecho Penal Informático en Venezuela"**. Universidad Dr. Rafael Belloso Chacin, Maracaibo, Venezuela.
- Haarscher A (2016) **"Delitos Informáticos".** Universidad Empresarial siglo 21, Bogotá, Colombia.
- Uzcategui, A. (2007) "**El comercio electrónico, los Delitos Informáticos y su Legislación Venezolana**". Universidad de los Andes, Mérida, Venezuela.