PROCEDIMIENTO PARA LA INVESTIGACIÓN DE LOS DELITOS RELACIONADOS CON LA DEEP WEB EN VENEZUELA

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS
ESCUELA DE DERECHO
CARRERA: DERECHO

PROCEDIMIENTO PARA LA INVESTIGACIÓN DE LOS DELITOS RELACIONADOS CON LA DEEP WEB EN VENEZUELA

Trabajo de Grado presentado como requisito para optar el título de Abogado

AUTOR:
González, Guillermo. C.I. 20.678766

TUTOR ACADÉMICO:
Prof. Luis Betancourt

San Diego, marzo 2020

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS
ESCUELA DE DERECHO
COORDINACIÓN DE PASANTÍAS

PROCEDIMIENTO PARA LA INVESTIGACIÓN DE LOS DELITOS RELACIONADOS CON LA DEEP WEB EN VENEZUELA

CONSTANCIA DE ACEPTACIÓN

_____

Prof. Luis Betancourt. C.I. 18.241.273. Tutor Académico

_____

Prof. Olga Matos. C.I. 8.470.308. Primer Jurado

_____

Prof. Jean Carlos Garrido. C.I. 17.192.837. Segundo Jurado

San Diego, marzo 2020

ÍNDICE GENERAL

AGRADECIMIENTOS

A mis **HIJOS** por ser el impulso que me llevó a estudiar esta carrera.

A mi **ESPOSA** que estuvo conmigo en todo momento a lo largo de mis estudios.

A mi **PROFESORES**, especialmente a Olga Matos, Carmen Luciana, Luis Armando Betancourt, Fabiana Morín, Ely Montañez, Argenis Flores.

REPÚBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JOSÉ ANTONIO PÁEZ

FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS

ESCUELA DE DERECHO

COORDINACIÓN DE PASANTÍAS

PROCEDIMIENTO PARA LA INVESTIGACIÓN DE LOS DELITOS RELACIONADOS CON LA DEEP WEB EN VENEZUELA

Autor:

Guillermo González

Tutor:

Prof. Luis Betancourt

Fecha:

Marzo 2020

RESUMEN INFORMATIVO

El presente trabajo de investigación se planteó como objetivo general determinar el procedimiento para la investigación de los delitos relacionados con la Deep Web en Venezuela. Esto conllevó a que se definieran tres objetivos específicos: (i) Identificar los delitos que pudieran realizarse mediante la Deep Web, (ii) Estudiar las bases legales para el procedimiento en los casos de delitos relacionados a la Deep Web y (iii) Recomendar el procedimiento a utilizar para la investigación de los delitos relacionados a la Deep Web. La metodología mediante la cual se abordaron tales objetivos fue a través de una investigación cualitativa de tipo descriptiva y explicativa bajo la revisión documental, cuyo método y técnica aplicada fue la recopilación de diferentes textos bibliográficos, normativos, legales y electrónicos, en los cuales se tomó en cuenta los criterios de actualidad para el análisis de contenido del presente trabajo. El trabajo permitió concluir que son numerosos los delitos informáticos que pudieran cometerse a través de la Deep Web para afectar los bienes jurídicos personales, como el ciberterrorismo, la pornografía infantil, lo delitos contra la propiedad intelectual, las estafas, subastas y ventas ilegales en Internet, entre otros. De la revisión a las bases legales para el procedimiento en los casos de delitos relacionados a la Deep Web se pudo verificar que no existe una legislación que haga referencia específica a este término, sin embargo algunos de los delitos fueron tipificados por la legislación especial, por lo que se recomendó aplicar el procedimiento establecido en el Convenio sobre la Cibercriminalidad.

Palabras Claves: Procedimientos, delitos, investigación, Deep Web.

INTRODUCCIÓN

Hoy día no se puede negar la importancia que tiene la tecnología en las vidas de los seres humanos. Gracias a ella se han logrado numerosos y significativos avances en diferentes contextos de la vida del ser humano, por lo que su impacto positivo para el desarrollo de las naciones es innegable.

Sin embargo, no todas las personas, hacen uso de dicha tecnología de manera positiva y casi a la par de su surgimiento, también empezaron a suscitarse situaciones que más adelante debieron ser catalogadas como delitos relacionados a la informática o delitos informáticos, que obligaron a los países del mundo a establecer tipificaciones en sus códigos penales o en leyes especiales creadas para tales efectos.

Por ello el presente trabajo aborda el procedimiento para la investigación de los delitos relacionados con la Deep Web en Venezuela, lo cual implicó la identificación de esos delitos que pueden ser realizados mediante la Deep Web, así como el estudio de las bases legales para el procedimiento de estos delitos, todo lo cual permitió el establecimiento de recomendaciones para ese procedimiento investigativo en el caso de Venezuela.

En consecuencia, para este trabajo de investigación, se estructuraron cuatro capítulos, en los cuales se desarrolló el planteamiento del problema, se esbozó el marco referencial conceptual, se describió la metodología utilizada y se presentaron los resultados, las conclusiones y las recomendaciones con base en los objetivos planteados.

CAPÍTULO I

EL PROBLEMA

1.1- Planteamiento del Problema

Las nuevas tecnologías de la información, su desarrollo y avance ha abierto las puertas al progreso, desarrollo y lo que es hoy considerado como un derecho humano, el acceso a la Internet y a todo el conocimiento alojado en la World Wide Web y sus diferentes programas y aplicaciones; no sólo a través de las computadoras, sino que también de la tecnología móvil que cada día se expande y pone en manos de miles de personas teléfonos de última generación con acceso a la Internet.

El desarrollo de estas nuevas tecnologías conlleva a reflexionar como señala Bautista (2014) “acerca del papel de los factores sociales, de la búsqueda de bienestar, de las prácticas que no tienen en cuenta el rostro de las personas”. En este orden, indica Castells (2001) que en Internet se pueden distinguir “dos agrupaciones: los que producen y a la vez utilizan internet y sus aplicaciones, retroalimentando el sistema, y quienes consumen y son usuarios de la red, que a la larga también terminan incidiendo de alguna manera en su evolución”.

Las nuevas tecnologías entonces han modificado el comportamiento de la sociedad a una velocidad vertiginosa que no se había experimentado hasta el momento, produciendo nuevos hábitos en los individuos, que adquieren una nueva identidad social como usuarios capaces de acceder, crear, compartir y modificar información y conocimiento.

En este contexto tan difícil para la aplicación de términos legales, no es extraño que ocurran irregularidades que cometen los usuarios en la actividad que llevan a cabo. La tecnología de la información puede ser utilizada tanto de manera positiva, como para cometer actividades delictivas, que entran dentro de ese mundo de los delitos informáticos.

La Deep web también conocida como web profunda o Internet profunda es uno de esos espacios a los que hace alusión el autor mencionado, en el cual se verifican distintos tipos de mercado que están a la orden de los usuarios. Dentro de esos sitios, algunos se pueden dedicar al cibercrimen o a realizar delitos informáticos. A tales efectos señala Bautista (2014) que esta Depp Web:

> "Es una parte gigantesca de las plataformas virtuales indetectables donde ocurren ciberacciones que tienen como precedente el ocultamiento de la identidad del usuario y han dado pie a la tergiversación del concepto de persona y a la utilización de la web de una manera irresponsable."

Para contrarrestar esta situación de criminalidad a través de las nuevas tecnologías, se han hecho múltiples esfuerzos para garantizar la seguridad informática, como por ejemplo en la mayoría de los países de Europa en los cuales se han adoptado legislaciones que tipifican y penalizan los actos delictivos que provienen del mal uso de la red. También a través de las Naciones Unidas (ONU), la Comunidad Europea y países como los Estados Unidos han llevado a cabo acciones, como la creación de órganos que analizan y proponen planes de acción que tienen que ver con el cibercrimen.

Pero esto ha resultado una tarea un tanto difícil, pues los autores de este tipo de delitos, se amparan en la tecnología que cada día se desarrolla más y ello facilita el ejercicio de las actividades delictivas, disponiendo en ese sentido de un mundo digital virtual y

anónimo que se caracteriza por ser indetectable, como lo es la Depp Web. Que como refiere Fernández (2015):

> "Se trata de un internet fuera de foco, no accesible a navegadores clásicos, que subyace bajo la red superficial que conocemos como internet. La Deep Web funciona gracias a una red global de usuarios de computadoras que creen que internet debería operar fuera de la supervisión de las agencias que vigilan el incumplimiento de la ley y se utiliza tanto con fines políticos como delictivos."

Muchos usuarios de la Internet se encuentran adaptados a espacios oscuros de la misma, en donde se puede descargar música de forma ilegal o encontrar películas que aún se transmiten en el cine, logrando no pagar por dichos accesos; pero la Depp Web constituye un nivel más alto en los índices de criminalidad, se trata de delitos mucho más graves como el tráfico de armas, intercambio de drogas, prostitución, pornografía infantil, terrorismo, entre otros actos.

Es oportuno aclarar en este punto, que no todos los usos de esta Deep Web se traducen en un delito o una irregularidad. Esta también sirve como refleja Fernández (2015) para aquellas personas que:

> "Encuentran sus libertades personales amenazadas, o que están siendo vigilados por organismos del gobierno. WikiLeaks es un caso emblemático de uno de los usos de la Deep Web, que durante mucho tiempo operó en ella. Otro caso también es el grupo Anonymous, que utilizan la red como punto de reunión y organización."

La Deep Web en palabras claras y sencillas constituye todos aquellos archivos que hay en Internet que no se encuentran indexados por los buscadores, es decir, las que están protegidas por una contraseña, como Facebook, las transacciones bancarias, Netflix, entre otras similares. Estas páginas protegidas se deben a que la información alojada en ellas sensible, y por tanto no debe ser de acceso público.

Ahora bien, tomando en cuenta lo anterior, el acceso a esta web profunda no necesariamente supone la comisión de un hecho punible, aunque algunos países como Austria, China, Egipto y Rusia, penalizan el uso y la tenencia de este tipo de navegadores específicos. Sin embargo, cuando se está frente a delitos tecnológicos la problemática viene dada por la característica de éstos en la dificultad de perseguir a los autores de los hechos, lo cual resulta aún más difícil cuando los actos ilícitos se cometen a través de la Deep Web. Aun así, hay países que cuentan con legislación para regular o limitar el acceso a la Internet o a páginas específicas de la red, pero no existe una regulación específica sobre el uso de navegadores que permiten el acceso a la Deep Web.

En Venezuela, existe un marco regulatorio de las telecomunicaciones que enmarca el acceso a la Internet, en el cual es necesario verificar si se encuentra defina la concepción, alcance e implicaciones de la Deep Web y si enumera, tipifica y sanciona los delitos asociados a la misma.

1.2.- Formulación del problema

En consecuencia a lo anteriormente planteado, se abren las siguientes interrogantes: ¿Existe un procedimiento aplicable a los delitos relacionados con la Deep Web en Venezuela? ¿Cuáles son los delitos que pudieran realizarse mediante la Deep Web? ¿Cuáles son las bases legales para el procedimiento en los casos de delitos relacionados a la Deep Web?

1.3.- Objetivos de la investigación

1.3.1.- Objetivo general

Determinar el procedimiento para la investigación de los delitos relacionados con la Deep Web en Venezuela.

1.3.2.- Objetivos específicos

- Identificar los delitos que pudieran realizarse mediante la Deep Web.
- Estudiar las bases legales para el procedimiento en los casos de delitos relacionados a la Deep Web.
- Recomendar el procedimiento a utilizar para la investigación de los delitos relacionados a la Deep Web.

1.4.- Justificación de la investigación

Las tecnologías de la información resultan hoy día una herramienta fundamental para el ser humano, no sólo desde el punto de vista laboral y académico, sino desde el punto de vista de la comunicación. Esta acerca a las personas que se encuentran lejanas, permite hacer transacciones bancarias a distancia, facilita el almacenamiento de información, entre otras funciones.

Sin embargo, como en todos los ámbitos de la vida del ser humano, el desarrollo de un bien o de un servicio se puede prestar no sólo para su uso positivo, sino también para el negativo. Es por ello, que se justicia la presente investigación para revisar si a través del uso de esas tecnologías y del acceso irregular a la Deep Web se producen implicaciones de tipo delictivo y si ello se encuentra debidamente tipificado en las leyes.

La Deep Webb o Internet profunda se ha convertido a lo largo del tiempo en un espacio poco explorado, que así como puede contener información de utilidad, también puede alojar contenidos que resulten devastadores para la sociedad, como en el caso de la pornografía o las redes de comunicación que han creado los terroristas. Entonces es necesario, no sólo dejar sentado que estos espacios pueden constituir una herramienta para el ejercicio de las libertades y derechos a la expresión y a la comunicación de los seres humanos, sino además que también se prestan para la comisión de actos que vulneran la seguridad y la integridad de las personas.

CAPÍTULO II

MARCO TEÓRICO

El marco teórico representa en el proceso de la investigación, el contexto teórico conceptual en el cual se presentan distintas teorías, conceptos, elementos y características, que le dan sentido a la investigación para su sustento, en base al problema planteado y el objeto en estudio. Es por ello que el marco teórico es de gran importancia para la investigación, no sólo porque da respuestas a las interrogantes, sino porque es la base conceptual que soportará el desarrollo de la investigación y el análisis de los resultados.

En tal sentido Arias (1999), señala que el marco teórico referencial, puede ser definido como “el compendio de una serie de elementos conceptuales que sirven de base a la indagación por realizar”. Bajo, esta perspectiva, resulta importante contar con un marco teórico que permita conocer las principales definiciones, elementos y características vinculadas al tema que se investiga y de esta manera tener como punto de referencia y constituir las bases fundamentales. Por su parte Balestrini (1998) afirma que el marco teórico: “es el resultado de la selección de aquellos aspectos más relacionados del cuerpo teórico epistemológico que asume, referidos al tema específico elegido para su estudio”.

2.1.- Antecedentes de la investigación

Los antecedentes reflejan los avances y el estado actual del conocimiento en un área determinada, sirviendo de modelo o ejemplo para futuras investigaciones. Según Arias (2004) se refieren a “todos los trabajos de investigación que anteceden al nuestro, es decir, aquellos trabajos donde se hayan manejado las mismas variables o se hallan

propuestos objetivos similares"; además sirven de guía al investigador y le permiten hacer comparaciones y tener ideas sobre cómo se trató el problema en esa oportunidad. Consiste entonces en la revisión de documentos contenidos de estudios que directa o indirectamente están relacionados con el problema de la investigación planteada. En este orden de ideas a continuación se mencionan los siguientes referentes:

Jiménez (2018) en su trabajo titulado **EL CONTEXTO JURÍDICO DE LA DEEP WEB**, presentado para la Universidad Rafael Landívar (Guatemala) para obtener el grado de Licenciado en Ciencias Jurídicas y Sociales, cuyo objetivo fue analizar el contexto jurídico que enmarca a la Deep Web y el impacto generado a nivel mundial y en particular en el medio guatemalteco, confrontándola con la normatividad vigente de dicho país.

De la revisión de este trabajo que se encuentra directamente relacionado al que aquí se presenta por abordar la noción jurídica tanto en el orden internacional y nacional de Guatemala, se concluye en primer lugar, que la Deep Web es un sitio en el cual se desarrollan relaciones sociales "en un espacio y tiempo determinado, en este caso la red virtual, razón por la cual pueden y deben quedar sujetas a los parámetros de la ley, bajo los postulados de certeza jurídica y justicia social".

En segundo lugar, que la libertad que da la Internet, permite la facilidad para la comisión de actividades ilícitas "por parte de usuarios malintencionados, que se valen de ello para cometer actos delictivos que con el pasar del tiempo hacen difícil su persecución penal". Y es por ello que el investigador menciona:

> "Es indispensable el surgimiento de normatividad especializada, donde concretamente se desarrolle una regulación efectiva en materia delitos informáticos, que busque sancionar a los sujetos que comentan los mismos, de manera que genere una protección íntegra hacia las personas y sus respectivos derechos."

Otro trabajo seleccionado en la búsqueda de información es el de Temperini (2018) titulado **DELITOS INFORMÁTICOS Y CIBERCRIMEN: ALCANCES, CONCEPTOS Y CARACTERÍSTICAS**, que fue presentado para la el suplemento especial Erreius (Argentina), con el objeto de explicar la "complejidad que representa un abordaje profundo de un tema tan importante como la ciberdelincuencia". Es por ello, que el autor realizó un repaso de algunos aspectos de la seguridad de la información, que considera imprescindibles al momento de comprender los argumentos a partir de los cuales giran los delitos informáticos. Además introdujo distintos conceptos tradicionales de la doctrina sobre delitos informáticos y cibercrimen, sus características generales y los desafíos que representan para el derecho.

Se define la Deep Web en esta investigación como el "espacio virtual más que existe en la actualidad, cada vez más accesible para los usuarios, y que posee determinadas características que es necesario considerar si se quiere hacer un estudio completo sobre los delitos informáticos" y agrega que "no es más que una parte de la red de Internet en la cual los contenidos no son indexados por los motores de búsquedas tradicionales (Google, Yahoo, Bing, etc.)".

Concluye entonces que no existe casi ninguna actividad en la cual no se incorpore para su realización un recurso digital o informático. Por tanto todo trabajo de investigación que se realice sobre medios digitales está supeditado:

> "A lo que se buscará y la manera de buscarlo. Ambas premisas (qué y cómo) incidirán en los tiempos de proceso, resultados de las búsquedas y un informe concluyente. Dicen que "la información es poder", pero la información contenida en medios digitales es estrechamente más poderosa. Por ello, se debe preservar su integridad, disponibilidad y confidencialidad, que son los paradigmas de la seguridad de la información."

Finalmente un tercer antecedente utilizado para este trabajo fue la revisión bibliográfica de Ortiz (2019) titulada **NORMATIVA LEGAL SOBRE DELITOS**

INFORMÁTICOS EN ECUADOR, que se propuso como objetivo fue efectuar una revisión general acerca del tema y comentar el estatus actual de la normativa jurídica que existe en Ecuador, sobre los delitos informáticos. Esta autora expone que:

> "Sin duda alguna, el uso de Internet facilita la vida de los usuarios, pero esos beneficios se tornan peligrosos cuando se infiltran entre los servicios del Internet programas maliciosos que de forma silenciosa pueden dañar no sólo los equipos tecnológicos sino también las finanzas de las personas, empresas y gobiernos."

Así mismo, esta investigadora comenta que los delitos informáticos en Latinoamérica se encuentran en crecimiento, pero, que "los países ubicados en esta región no tienen un marco legal homogéneo aplicable a los delitos de esta índole, por tal motivo es complicado combatirlos".

En este orden concluye que:

> El robo, hurto, estafa, pornografía, contrabando, entre otros delitos tradicionales, en la actualidad se realizan a través del uso de herramientas informáticas y del Internet. Estos delitos son cometidos por delincuentes que tienen un buen dominio en el uso de las TIC. Los delitos más graves como el narcotráfico, trata de blancas y pornografía infantil son cometidos en la Internet profunda, también llamada Internet oscura.

2.2.- Bases teóricas

Haciendo referencia a las bases teóricas, representan el compendio de una serie de elementos conceptuales que sirven de base a la indagación en desarrollo. Es decir, que comprenden un conjunto de conceptos y proposiciones que constituyen un punto de vista o enfoque determinado, dirigido a explicar el fenómeno o problema planteado.

Delitos informáticos

Existen numerosas definiciones respecto a los delitos informáticos, como la de Hernández (2009), quien lo considera como:

> Toda acción dolosa que provoca un perjuicio a personas o entidades, sin que necesariamente conlleve un beneficio material para su autor aun cuando no perjudique de forma directa o inmediata a la víctima y en cuya comisión intervienen necesariamente de forma activa dispositivos habitualmente utilizados en las actividades informáticas.

Una definición más simple la proponen Loredo y Ramírez (2013), quienes exponen que: “Delito informático es el uso de cualquier sistema informático como medio o fin de un delito”. Con esta definición abarcan cualquier tipo delictivo que pueda haber sido establecido en un marco legal de un país.

En este orden de ideas, conviene definir qué es un sistema informático. De acuerdo con el Convenio sobre la Ciberdelincuencia (2001) se debe entender por este a “todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa". En esta definición no sólo se abarca a las computadoras, sino a cualquier sistema que permita la ejecución de un programa o la manipulación de datos. Por otra parte, la Secretaria de Seguridad Pública (2012) de México define el delito cibernético como: “Actos u omisiones que sancionan las leyes penales con relación al mal uso de los medios cibernéticos.”

Ahora bien, existen diversas posturas doctrinarias que conceptualizan a los denominados delitos informáticos. Se mencionarán las cuatro posturas más resaltantes en base a los elementos comunes que las integran. A continuación entonces las diferentes posturas:

a) *Elemento común: la utilización de la informática como método, medio o fin, de una conducta ilícita*

Las primeras definiciones que pretendieron delimitar el campo de estudio y a su vez conceptualizar el término delitos informáticos, consideraron que de manera general, cualquier acto penalmente perseguible que ha utilizado a la informática como método o instrumento; o bien que la misma ha sido el objeto o fin de dicha conducta, podría ser enmarcado dentro del campo de estudio de los denominados delitos informáticos. De esta manera se mencionan tres autores que integran esta postura:

Sarzana (citado por Tellez, 1998) delimita a los delitos informáticos como "cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo". Mientras que el propio Tellez (1998) los define como "las conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin".

Lima (citada por Marquez, 2003) considera que los delitos electrónicos en un sentido amplio son "cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica, ya sea como método, medio o fin" y en su sentido restringido el delito informático es "cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel, ya sea como método, medio o fin".

b) *Elemento común: la información o los daos procesados electrónicamente como bien protegible en los delitos informáticos*

Esta teoría separa en dos los tipos delictuales: los ya tipificados (que constituyen figuras normales y ordinarias del derecho penal, figuras delictivas clásicas) y los verdaderamente nuevos, que surgen por las nuevas condiciones que generan la informática y la sociedad de la información.

La definición dada por los autores que defienden esta postura sobre los delitos informáticos es la siguiente:

> "Toda conducta que revista características 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."

Los autores establecen, que el bien jurídico afectado por los delitos informáticos es la información que se encuentra almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos. Es por ello, que se ha clasificado dentro de estas posturas a los ilícitos informáticos en: a) conductas lesivas a la confidencialidad de la información, b) conductas lesivas a la integridad de la información y c) conductas lesivas a la disponibilidad de la información.

c) Elemento común: la negación de la existencia de estos delitos

Algunos doctrinarios se han negado al reconocimiento de la existencia de estos delitos, porque para ellos no constituye una nueva categoría delictiva. Los hechos ilícitos que se cometen o facilitan mediante el empleo de una computadora, son los mismos que se han realizado siempre. Sin embargo, ello no significa que nieguen el impacto de las nuevas tecnologías en la sociedad y la necesidad de reformar las normas penales para adecuarse a estos cambios.

d) Teoría ecléctica

Finalmente, se encuentran autores que consideran que si bien pudiesen existir delitos informáticos, el bien jurídico afectado aún no está delimitado y en cualquier caso ello no incluiría conductas que puedan encuadrarse en tipos penales clásicos.

Tipos delitos informáticos

Los delitos informáticos abarcan múltiples modalidades como se mencionan en la web de la Organización Internacional de Policía Criminal (INTERPOL) que se enumeran a continuación:

1. Ataques contra sistemas y datos informáticos.
2. Usurpación de la identidad.
3. Distribución de imágenes de agresiones sexuales contra menores.
4. Estafas a través de Internet Intrusión en servicios financieros en línea.
5. Difusión de virus.
6. *Botnets* (redes de equipos infectados controlados por usuarios remotos).
7. *Phishing* (adquisición fraudulenta de información personal confidencial).

También existen riesgos relacionados con el uso de las redes sociales y acceso a todo tipo de información, que mencionan Loredo y Ramírez (2013) tales como:

1. Acceso a material inadecuado (ilícito, violento, pornográfico, etc.).
2. Adicción - Procrastinación (distracciones para los usuarios).
3. Problemas de socialización.
4. Robos de identidad Acoso (pérdida de intimidad).
5. *Sexting* (manejo de contenido erótico).

6. *Ciberbullying* (acoso entre menores por diversos medios: móvil, Internet, videojuegos, etc.).
7. *Cibergrooming* (método utilizado por pederastas para contactar con niños y adolescentes en redes sociales o salas de chat).

En Venezuela, se realiza una clasificación de delitos previstos por el ordenamiento jurídico nacional en materia de delitos informáticos, sea que la informática es el medio, o que se tiene a la misma como fin u objeto, o tengan que ver con los derechos intelectuales o las llamadas nuevas creaciones jurídicas con respecto a los delitos informáticos.

1. *Delitos tradicionales que utilizan a la informática como medio*:

1.1. Hurto.
1.2. Violación a la privacidad de las comunicaciones.
1.3. Violación a la privacidad de la data o la información.
1.4. Difamación e injuria.
1.5. Difusión de informaciones falsas.
1.6. Delitos relativos a los niños, niñas y adolescentes:
1.6.1. Falta de advertencias o avisos preventivos.
1.6.2. Acceso de menores de edad a contenidos restringidos.
1.6.3. Creación de materiales pornográficos para su publicación o distribución por cualquier medio.
1.6.4. Distribución o difusión de imágenes de menores con fines exhibicionistas o pornográficos.

2. *Delitos tradicionales que tienen a la informática como fin u objeto*:

2.1. Sabotaje o daño a sistemas.
2.2. Falsificación de documentos.

3. *Delitos contra los derechos intelectuales*:

3.1. Reproducción no autorizada de una obra protegida.

3.2. Comunicación pública no autorizada.

3.3. Distribución no autorizada de obras lícitas.

3.4. Distribución no autorizada de fonogramas.

3.5. Retransmisión no autorizada de una emisión de radiodifusión.

4. *Delitos que constituyen o pueden constituir nuevas creaciones jurídicas*:

4.1. Acceso indebido.

4.2. Posesión de equipos o prestación de servicios de sabotaje.

4.3. Fraude informático.

4.4. Oferta engañosa.

4.5. Delitos relativos a las tarjetas inteligentes.

Concepto y generalidades de la Deep Web

La Internet nos permite acceder a una enorme cantidad de información de todo tipo. Loredo y Rodríguez (2013) mencionan que "los proveedores de este servicio siempre buscan mantener fuera de sus resultados el contenido no apto para el usuario". Pero fuera de ese contenido indexado existe otra parte de la red, conocida como Deep Web o Internet profunda, que estos mismo autores definen como:

> El conjunto de sitios que contienen material potencialmente peligroso para el usuario, no solo de índole sexual, también existen, videos *snuff* (grabaciones de asesinatos, violaciones, torturas y otros crímenes reales), mercado negro *online* (tráfico de armas, drogas, trata de personas, etc), contratación de asesinos, no existen límites para la gravedad del contenido que se puede encontrar.

Para Bautista (2014) “la Deep web es el contenido secreto de Internet que no está visible para los usuarios y que requiere vías distintas a los servidores tradicionales para llegar a sus contenidos que no siempre son adecuados para las personas”.

En consecuencia se trata de espacios en los cuales distintos tipos de mercado están a la orden de los usuarios. Aunque, no se puede afirmar que todos los sitios estén dedicados al cibercrimen, sin embargo, es necesario analizar lo que acontece allí, teniendo en cuenta que existen repercusiones sociales, políticas, económicas y jurídicas del uso del ciberespacio.

Por su parte la Asociación de Internautas (2020) la denomina también como Internet Invisible que:

> Engloba toda la información que se encuentra en la Web, pero que no se haya indexada por los motores de búsqueda tal y como los conocemos. Se trata, por tanto, de todo el contenido público online que no es rastreado ni encontrado por el usuario de a pie en la red.

Huay (2016) identifica diferentes niveles de dicha Deep Web, porque señala que todas las páginas web existentes se pueden clasificar en diferentes niveles de acuerdo a su contenido. Específicamente identifica cinco niveles que se explican a continuación:

> **Nivel 0.** Conocido como el “nivel superficial”, es el que todos conocemos y usamos día a día, y que actualmente dominan el mundo internauta, tales son Google, Youtube, y páginas similares; en este nivel es donde existe más censura y el contenido prohibido es eliminado.
> **Nivel 1**. Conocido como “Bergie”. Aquí se encuentra las páginas web un poco menos conocidas pero de fácil acceso, en su mayoría foros, páginas pornográficas y pequeñas páginas independientes de interés no tan común como en el nivel anterior; cabe destacar que el nivel de censura disminuye conforme se adentra más y más en el submundo.
> **Nivel 2**. Está compuesto por buscadores independientes, en los cuales podemos encontrar información dudosa, donde el morbo es tendencia en este nivel, estos buscadores pueden ser tales como el Utorrent, Emule,

> Ares… etc. También su acceso es simple y sencillo, el interés de cada uno de estos buscadores es la descarga.
> **Nivel 3**. Conocido como “Deep”, a partir de aquí las cosas cambian radicalmente, el primer cambio que surgirá seria los links o direcciones URL, ya que estos dejarían de terminar en “.com” y serían reemplazados por el Pseudodominio “.onion”. Además sería necesaria la utilización de un proxy.
> **Nivel 4**. Conocido como “Charter”. Siempre hay que tener el ordenador preparado para cualquier “amenaza hacker”. El cuarto nivel está plagado de hackers, refiriéndonos a verdaderos piratas informáticos, dedicados al robo, espionaje y a la malversación de datos. En este nivel, existe lo que se llama Snuff, es decir, grabaciones o en vivo de mutilaciones y asesinatos reales y; principalmente el “Mercado Negro”, donde existe la venta y tráfico ilegal de drogas, armas, órganos, e incluso contratación de sicarios.
> También en este nivel es posible encontrar páginas encriptadas de muchos gobiernos, donde se puede observar información sobre el destino del dinero de esos países, además existen documentos secretos de estado y los famosos Wikileaks que salieron al conocimiento de las personas con el caso de Julian Assange.
> **Nivel 5**. Conocido como “Marianas”. Para acceder a este nivel se requieren conocimientos en mecánica (o física) cuántica y algún programa o, componente llamado "PolymericFalcigholDerivation". En este nivel se exhiben los verdaderos planes para las economías mundiales, unificación de gobiernos y lo que nos oculta el Estado como la entidad que realmente domina el mundo.

A diferencia del autor anterior, la Asociación de Internautas (2020) identifica los siguientes niveles:

> Web Visible: son todas aquellas páginas comunes que visitamos en nuestro día a día navegando por la red.
>
> Buscadores.
>
> Redes Sociales.
>
> Páginas web de diversa índole (informativas, blogs, canales de entretenimiento).
>
> Web Invisible: aquellas páginas que no son rastreadas por los buscadores tradicionales.
>
> Páginas de descargas piratas, como los torrents y de descarga masiva.
>
> Foros Onion Chan, portales de pornografía infantil, venta de objetos robados, tráfico de armas.

> Sitios de extremistas, grupos ilegales, de revolucionarios, etc.
>
> Redes gubernamentales, sitios web de acceso restringido, programas de espionaje.

Ahora bien, es posible determinar cómo puede una web terminar alojada en la Deep Web. En primer lugar, esto se debe a que los contenidos que estén publicados en la misma, se encuentren en un formato no indexable (es decir, ilegible) para los motores de búsqueda tradicionales; y en segundo lugar, la página puede estar protegida con contraseña o sistemas de CAPTCHA que evitan que los rastreadores accedan a su contenido (Asociación de Internautas, 2020).

El navegador web The Onion Router o TOR, según González (2015):

> Es el más popular para acceder a la Internet Profunda. La estructura y funcionamiento de esta red descentralizada de ordenadores funciona según nodos, que son los componentes de la misma encargados de eliminar el rastro de navegación. De forma simple, estos nodos son los intermediarios en el tráfico de intercambio de datos, y los responsables, hasta cierto punto, de nuestra velocidad de navegación usando Tor. Razón por la cual existe la posibilidad de eliminar el rastro de tráfico de intercambio en la navegación por Internet.

La naturaleza entonces de la Deep Web permite la realización de actividades ilícitas en su mayoría, lo que ha conllevado a ser el punto de partida para desarrollar estructuras criminales con el fin de contar con una facilidad y beneficios para realizar una serie de delitos.

Según García (2016) “la parte más oscura de la Deep Web se conoce como la darknet. En ella, es donde se hallan los supermercados de drogas y armas, así como casi cualquier otro espacio de actividades ilegales que se pueda imaginar”. Agrega que se trata de un tipo de páginas de acceso muy restringido cuyo contenido está cifrado

siempre, y que cambian a menudo de ubicación. Para acceder a ellas, explica que "además de ser intrépido (o incauto), sería necesario tener conocimientos informáticos superiores al usuario medio de internet. Por ejemplo, para crear una cartera de bitcoins, que es la moneda de curso legal para realizar transacciones en la deep web".

2.3.- Bases legales

El marco legal nacional e internacional aplicable a los delitos informáticos cometidos en Venezuela está constituido por diferentes normas dependiendo del delito que se haya cometido. Con la entrada en vigencia de la Constitución Nacional de 1999, se ha definido un marco regulatorio de las telecomunicaciones en Venezuela y, más específicamente, del acceso a internet.

Tomando en cuenta lo anterior, si se trata de delitos tradicionales que utilizan como medio a la informática, se pueden cometer hurtos los cuales están tipificados de forma general en el Código Penal venezolano y de manera específica en la Ley Especial contra Delitos Informáticos. También se verifican violaciones a la privacidad de las comunicaciones contempladas en la Ley Especial contra Delitos Informáticos.

En el caso de las violaciones a la privacidad de la data o información, la Ley Especial contra Delitos Informáticos prevé tres conductas delictivas en ese sentido. E igualmente el Código Penal venezolano lo tipifica como delito. También se pueden cometer delitos utilizando a la informática como medio, como lo son la difamación y la injuria tipificados en el Código Penal venezolano. O la difusión de informaciones falsas que de igual forma está regulada en el referido Código.

Ahora bien, en los delitos relativos a niños, niñas y adolescentes se debe verificar lo establecido en la Ley Orgánica para la Protección de Niños, Niñas y Adolescentes, la

Ley para la Protección de Niños, Niñas y Adolescentes en Salas de Uso de Internet, Videojuegos y otros Multimedias, que reguló el acceso de niños y adolescentes a contenidos prohibidos y la Ley para la Prohibición de Videojuegos y Juguetes Bélicos, la reforma a la Ley de Responsabilidad Social en Radio y Televisión de 2010, y la llamada Ley contra el Odio.

En otro orden, en los delitos tradicionales que tienen a la informática como fin u objeto, igualmente resaltan como marco legal el Código Penal venezolano y la Ley Especial contra los Delitos Informáticos. Los delitos que se pueden cometer dentro de esta clasificación son el sabotaje o daños a sistemas y la falsificación de documentos.

Por otro lado, en los delitos contra los derechos intelectuales, el marco legal en este caso es la Constitución de la República Bolivariana de Venezuela, la Ley Sobre Derechos de Autor y la Ley de Propiedad Industrial. Y finalmente, en los delitos que constituyen o pueden constituir nuevas creaciones jurídicas, el marco legal está constituido por el Código Penal y la Ley contra Delitos Informáticos.

Ahora bien, entendiendo que la Deep Web ha sido considerada como un lugar inseguro, que no ofrece seguridad o protección directa hacia los usuarios, esta ha sido considerada una de las causas por las que se cometen actos delictivos que generan impacto en el mundo real. El alcance de las actividades delictivas en la red se incrementa con el paso del tiempo debido a la gran cantidad de herramientas que surgen para la ayuda en la perpetración los delitos informáticos.

Flores (2014) señala al respecto que “el derecho penal de los estados interesados en combatir esta nueva delincuencia, contiene vacíos jurídicos y diferencias importantes susceptibles de obstaculizar la lucha contra la delincuencia organizada y el terrorismo, así como los graves ataques contra sistemas de información perpetrados por particulares”.

De allí que se determine que la cooperación internacional es clave para brindarle una solución a la problemática de esta criminalidad moderna. Con el fin de apoyar la cooperación internacional se han creado normativas jurídicas internacionales que permiten la regulación de la plataforma informática para evitar la realización de ilícitos.

Por ello, el Consejo de Europa, adopta el Convenio de Ciberdelincuencia en el año 2001, conocido también como el Convenio de Budapest. Las conductas ilícitas reguladas en el Convenio son: el acceso ilegal, interceptación ilegal, interferencia de los datos, interferencia del sistema uso erróneo de dispositivos, falsificación del ordenador, fraude del ordenador y pornografía infantil. También describe los elementos que deben tomar en cuenta las legislaciones del derecho interno referentes a los delitos informáticos, así como los procesos y competencias para la persecución penal de estos delitos.

Alvarado y Morales (2012) comentan que, el Convenio de Budapest, a pesar de ser celebrado por el Consejo de Europa, no tiene algún tipo de impedimento legal para que otros países puedan adherirse a dicha normativa.

Por su parte, la Organización de Naciones Unidas ha desarrollado estrategias y normativas para la regulación de actividades informáticas. Algunas de ellas son: La Declaración de Viena sobre la Delincuencia y la Justicia frente a los retos del siglo XXI, el Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos, el Tratado de la Organización Mundial de la Propiedad Intelectual Sobre el Derecho de Autor, el Convenio de Berna sobre los Derechos de Autor, La Convención para la Protección y Producción de Fonogramas, el Convenio de París para la Propiedad Industrial, entre otros.

2.4.- Definición de términos básicos

Según Tamayo (1995) la definición de términos, es "…la aclaración del sentido en que se utilizan las palabras o conceptos empleados en la identificación y formulación del problema". Es decir aquellos que aclaran el significado de las palabras o concepciones inmersas en el problema.

Computador: dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas.

Datos informáticos. Cualquier representación de hechos, información o conceptos de una forma que permita el tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función.

Documentos. Son todo tipo de archivos de texto como documentos políticos, documentos secretos, documentales que no son públicos, blogs, comunidades grandes, leyes, decretos, patentes, diccionarios, bibliotecas, librerías, periódicos, páginas amarillas, Sitios de empresas, bases de datos, wikileaks (filtración de información), manuales para robar bancos, manuales de guerrilla, guías y listas de teléfonos.

Información: significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

Seguridad: Condición que resulta del establecimiento y mantenimiento de medidas de protección que garanticen un estado de inviolabilidad de influencias o de actos hostiles

específicos que puedan propiciar el acceso a la data de personas no autorizadas o que afecten la operatividad de las funciones de un sistema de computación.

Sistema: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

Sistema informático. Todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa.

Tecnología de Información: rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, 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 data.

CAPÍTULO III

MARCO METODOLÓGICO

Una vez ubicado el objeto de estudio de la investigación en su contexto teórico conceptual, se hace necesario abordar el aspecto metodológico, que se refiere a los distintos métodos empleados; esto se hace a los fines de validar los resultados obtenidos en la aplicación de instrumentos y/o técnicas de recolección de datos que concluirán con el proceso investigativo, tras la presentación de los resultados y su respectivo análisis. Es por ello, que en este capítulo denominado marco metodológico se describirá en forma precisa los componentes de la metodología, es decir, el procedimiento que se utilizó en la realización de la investigación para alcanzar los objetivos propuestos.

El marco metodológico según Balestrini (2001): “es la instancia referida a los métodos, las diversas reglas, registros, técnicas y protocolos con los cuales una Teoría y su Método calculan las magnitudes de lo real…”. En tal sentido, la metodología está referida al plan básico que se sigue al realizar la investigación.

Según Arias (1999), “la metodología incluye el tipo o tipos de investigación, las técnicas y los procedimientos que serán utilizados para llevar a cabo la indagación”. Es decir que, es el cómo se realiza el estudio para responder al problema planteado.

3.1- Tipo de investigación

De acuerdo al problema planteado y en función a los objetivos específicos, la presente investigación se ubica dentro de la modalidad de una investigación cualitativa de tipo descriptiva y explicativa bajo la revisión documental.

En tal sentido, señala Balestrini (2001), que los estudios descriptivos infieren "…acerca de las singularidades de una realidad estudiada, podrá estar referida a una comunidad, una organización, un hecho delictivo, características de un tipo de gestión, conducta de un individuo o grupales…etc.". Es decir, independientemente se selecciona una serie de cuestiones, se mide cada una de ellas y así se descubre lo que se investiga. Por otra parte, los autores Hernández, Fernández y Baptista (2000) se refieren al método descriptivo como: "la búsqueda especifica de características, propiedades y rasgos importantes de cualquier fenómeno que se analice".

3.2- Métodos y técnicas de la investigación jurídica

Como técnica para la obtención de la información documental, se utilizó una recopilación de diferentes textos bibliográficos, normativos, legales y electrónicos, en los cuales se tomó en cuenta los criterios de actualidad para el análisis de contenido del presente trabajo, lo que le permitió a los investigadores desarrollar los objetivos propuestos y diferentes capítulos, cuyos textos sirvieron para describir las bases teóricas-jurídicas y fundamentar esta investigación documental.

Por otra parte, Ander (1988) señala que: "existe una amplia variedad y diversidad de documentos utilizables para una investigación. Pueden distinguirse entre documentos escritos, documentos numéricos o estadísticos, documentos cartográficos, documentos de imagen y sonido, y documentos objeto".

Al respecto Sabino (2000), señala lo siguiente: "llámese análisis de contenido a una técnica de investigación que se basa en el estudio cualitativo del contenido manifiesto de la comunicación". Igualmente se utilizó la observación documental a través de la lectura evaluativa, así como la técnica de fichaje y de resúmenes.

En cuanto a la observación documental, Balestrini (2002) señala que: “esta se utiliza como punto de partida en el análisis de las fuentes documentales, mediante una lectura general de los textos, se iniciará la búsqueda y observación de los hechos presentes en los materiales escritos consultados que son de interés para esta investigación”. Por otra parte, la lectura evaluativa se entiende como aquella lectura que según Alfonso (1999):

> Es esencialmente crítica, pues, no se trata sólo de comprender el pensamiento de un autor, sino de valorarlo, la lectura que se realiza para la recolección de los datos tiene un carácter sumamente complejo, ya que la misma constituye el nivel más difícil que puede alcanzarse en la actividad de leer.

De la misma forma, se emplea la técnica de resúmenes, que según Alfonso (1999): se define como: “la exposición condensada de un escrito en el cual se refleja fielmente las ideas expresada en el texto original, su extensión es variable, pues puede referirse desde un párrafo hasta un libro”.

Y por último, como instrumento de ayuda para facilitar la recopilación y clasificación de la información, se utilizó las fichas de trabajo, las cuales permitieron una mejor organización de la información extraída de las fuentes consultadas, pudiéndose utilizar adicionalmente entre otras, la técnica del subrayado.

3.3- Fases de la investigación

Fase I. Identificar los delitos que pudieran realizarse mediante la Deep Web.

Fase II. Estudiar las bases legales para el procedimiento en los casos de delitos relacionados a la Deep Web.

Fase III. Recomendar el procedimiento a utilizar para la investigación de los delitos relacionados a la Deep Web.

3.4.- Fuentes del conocimiento

a. Doctrina
b. Legislación
c. Realidad socio-jurídica.

CAPÍTULO IV

RESULTADOS, CONCLUSIONES Y RECOMENDACIONES

4.1- Resultados y conclusiones

Identificar los delitos que pudieran realizarse mediante la Deep Web.

Son numerosos los delitos informáticos que pudieran cometerse a través de la Deep Web para afectar los bienes jurídicos personales, sin embargo se presentan dentro de estos resultados los que a juicio de la doctrina, la investigación y la opinión de expertos generan mayores pérdidas económicas y sociales a nivel internacional:

1. Ciberterrorismo:

Definido por De la Corte y Blanco (2014), como aquellas acciones ofensivas que se planifican y se realizan en contra de gobiernos, Estados, sectores de población determinados o poblaciones enteras con el fin de coaccionar e intimidar o generar un profundo impacto psicológico. Señalan que “esto afectaría a la información, sistemas, programas, datos informatizados e infraestructuras críticos”.

Los ciberterroristas hacen uso de las tecnologías de la comunicación e información para cometer sus delitos. La oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, 2013) establece que los grupos terroristas utilizan el Internet para realizar las siguientes tareas: “la propaganda (incluidos el reclutamiento, la radicalización y la incitación al terrorismo); la financiación; el adiestramiento; la planificación (por medio

de comunicaciones secretas o de dominio público); la ejecución; y los ataques cibernéticos".

2. Pornografía Infantil:

El convenio de Budapest define a la pornografía infantil como todo aquel material pornográfico que "contenga la representación visual de un menor comportándose de una forma sexualmente explícita; una persona que aparezca con un menor comportándose de una forma sexualmente explicita"; así como imágenes "realistas que representan a un menor comportándose de una forma sexualmente explícita".

Es oportuno destacar en este punto que cada país define qué debe entenderse por menor, como por ejemplo en el caso de Venezuela que tanto el Código Civil, como la Ley Orgánica para la Protección del Niño, Niña y Adolescente, así como la Constitución Nacional como norma suprema y el Convenio de los Derechos del Niño suscrito y ratificado por el Estado venezolano, coincide en catalogar que son menores de edad, los que tengan menos de 18 años.

De igual forma en el Convenio se establecen los delitos relacionados con la pornografía infantil. Estos son:

a) La producción de pornografía infantil con vistas a su difusión por medio de un sistema informático;

b) La oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;

c) La difusión o transmisión de pornografía infantil por medio de un sistema informático;

d) La adquisición de pornografía infantil por medio de un sistema informática para uno mismo o para otra persona;

e) La posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

Ruiz (2017) afirma que hoy en día la pornografía infantil es uno de los negocios que genera más dinero en la red, pues el Internet ha permitido su fácil expansión y ha limitado la identificación y localización de los responsables de este hecho delictivo. “Según un estudio realizado por la Universidad de Porstmouth, el 80% del tráfico generado en la 'deep web' está relacionado con sitios web de pornografía infantil” (Tecnoxplora, 2015).

3. Delitos Contra la Propiedad Intelectual:

La propiedad intelectual está referida a todas las obras del ingenio, del intelecto humano que son susceptibles de protección. Se divide en dos grandes ramas que son la del derecho de autor, dentro de la cual se ubican las obras literarias y artísticas y sus derechos conexos; y la segunda rama, la propiedad industrial en la que se encuentran reguladas las marcas, patentes, nombres comerciales, lemas comerciales, entre otra figuras (Organización Mundial de la Propiedad Intelectual, 2018).

Los autores de sus obras (derecho de autor) tienen derechos sobre las mismas relacionados como explica Moisés (2018) con la reproducción (capacidad exclusiva de autorizar la duplicación), la distribución (autorización a un tercero para la puesta a disposición del público del original o copias), la comunicación pública (el autoriza el número de personas que pueden ingresar a la obra) y la transformación (autorizar posibles trabajos derivados de la obra).

Ortiz (2019) opina que las leyes que protegen la propiedad intelectual son insuficientes y no pueden amparar las obras en el nuevo marco de la sociedad de la información e Internet. El Internet les ha permitido a los autores generar muchas ganancias, facilitando la mayor distribución de sus obras; sin embargo, la red no permite al autor controlar el número de copias o reproducciones que se hacen de su obra.

4. Delitos de calumnias e injurias:

La Internet permite que se difundan de forma masiva y universal las difamaciones, calumnias e injurias. Este delito e configura cuando se le da publicidad a ofensas e insultos que se mencionan sobre una persona, descalificándola, y resultan más graves que en aquellos casos en que se comete el delito sin que medie la internet, debido a que el contenido difamatorio se extiende de forma rápida y casi incontrolable por todas las redes sociales. Por ello acota García (2015): “Cuando alguien se excede en el ejercicio de su libertad de expresión entramos en el ámbito del delito".

5. Las estafas, subastas y ventas ilegales en Internet:

Las estafas electrónicas en palabras de Iglesis (2018) consisten “en la manipulación informática o artificio similar que, concurriendo ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero”. Según Oxman (2013) el *phising*, *pharming* y el *money mules* son formas de estafas informáticas que se dan en la red.

A través del *phishing* los delincuentes obtienen los datos personales y/o financieros de la víctima por medio del envío masivo de correos electrónicos con enlaces a páginas web falsas en las que se imita el contenido o la imagen de una entidad financiera o bancaria.

El *pharming* utiliza otro tipo de mecanismo para realizar las estafas, pues en este caso los malhechores manipulan las direcciones DNS que son utilizadas por el usuario redireccionando a éste a la navegación de sitios web que son falsos y han sido creados con el objetivo de defraudar.

En último lugar, el *money-mules* hace referencia a una conducta de colaboración que opera con posterioridad a la consumación de la defraudación patrimonial. Ella consiste, esencialmente, en poner a disposición de los estafadores (*scammers*) el dinero obtenido por éstos a través del *phishing* o *pharming*.

BBC Mundo (2017) plantea que las ventas ilegales de artículos y su fácil obtención, se dan ampliamente en la Deep Web. Los cibercriminales, ciberterroristas, hackers, entre otros tipos de delincuentes, son los que navegan por la Deep Web para cometer sus actos dolosos. Los cinco productos más vendidos son drogas, armas, identificaciones y dinero falso, software para hacker y pornografía infantil.

Estudiar las bases legales para el procedimiento en los casos de delitos relacionados a la Deep Web.

Tomando en cuenta los delitos informáticos antes referidos ciberterrorismo, pornografía infantil, delitos contra la propiedad intelectual, calumnias, injurias y las estafas, subastas y ventas ilegales en Internet, se debió revisar la legislación venezolana para determinar si los mismos se encuentran en primer lugar tipificados como delitos asociados a la informática y cómo se regulan.

Se verificó en ese sentido, que dentro de la clasificación que se realizó en este trabajo, se ubica la violación a la privacidad de la data o la información, la difamación e injuria,

la difusión de informaciones falsas, los delitos relativos a los niños, niñas y adolescentes, la creación de materiales pornográficos para su publicación o distribución por cualquier medio y la distribución o difusión de imágenes de menores con fines exhibicionistas o pornográficos; dentro de los delitos tradicionales que utilizan a la informática como medio para cometer el acto delictivo.

A tales efectos la Ley Especial de Delitos Informáticos establece en su artículo 20, que la violación de la privacidad de la data o información de carácter personal se entiende como la actuación de aquel que por cualquier medio se apodere, utilice, modifique o elimine, 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.

En el artículo 23 se hace alusión a la difusión o exhibición de material pornográfico. Expresa este artículo que el que por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda libremente, de modo que pueda ser accedido por niños o adolescentes, material pornográfico o reservado a personas adultas, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Y sobre la exhibición pornográfica de niños o adolescentes, estipula el artículo 24 que se trata de aquella persona que por cualquier medio involucre el uso de tecnologías de información, que utilice a la persona o imagen de un niño o adolescente con fines exhibicionistas o pornográficos.

En cuanto a los delitos que se cometen contra los derechos intelectuales, estos pueden ser la reproducción no autorizada de una obra protegida, la comunicación pública no autorizada, la distribución no autorizada de obras lícitas, la distribución no autorizada de fonogramas y la retransmisión no autorizada de una emisión de radiodifusión.

El artículo 25 de la comentada que apropiación de propiedad intelectual es aquellas que, 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.

Finalmente, dentro de los delitos que constituyen o pueden constituir nuevas creaciones jurídicas se encuentran el acceso indebido, el fraude informático y la oferta engañosa. Este acceso indebido, está tipificado como un delito y es definido por el artículo 6 de la Ley Especial contra los Delitos informáticos, haciendo referencia a aquellos que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información.

En cuanto a la oferta engañosa, el artículo 26 refiere al 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.

De la revisión a las bases legales para el procedimiento en los casos de delitos relacionados a la Deep Web se pudo verificar que no existe una legislación que haga referencia específica a este término, sin embargo algunos de los delitos fueron tipificados por la ley comentada, a excepción del ciberterrorismo y las ventas ilegales de drogas, armas, identificaciones y dinero falso y software para hacker usando como medio a la Internet.

Aunado a lo anterior, Venezuela tampoco es firmante del Convenio sobre Cibercriminalidad de Budapest. En América lo han suscrito y ratificado solamente Argentina, Canadá, Chile, Costa Rica, Panamá, Paraguay, República Dominicana y Estados Unidos.

Recomendar el procedimiento a utilizar para la investigación de los delitos relacionados a la Deep Web.

Tomando en cuenta lo expresado en el resultado anterior y aun cuando Venezuela no sea parte del Convenio sobre la Cibercriminalidad, es oportuno para efectos de poder recomendar el procedimiento a utilizar para la investigación de los delitos relacionados a la Deep Web, verificar el contenido de este Convenio.

En primer lugar, el artículo 14 establece que cada parte debe adoptar las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos para los fines de investigaciones o procedimientos penales específicos.

En este sentido, cada parte debe adoptar medidas legislativas y administrativas necesarias para que los delitos tengan sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad y sanciones pecuniarias, a las personas jurídicas consideradas responsables de los mismos.

El establecimiento, la ejecución y la aplicación de los poderes y procedimientos deben estar sujetos a las condiciones y salvaguardas previstas en el derecho interno venezolano, que debe garantizar una protección adecuada de los derechos humanos y de las libertades. Estas condiciones pueden incluir la supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen la aplicación, y la limitación del ámbito de aplicación y de la duración del poder o del procedimiento de que se trate.

Además, se debe tener presente el principio de cooperación internacional en materia penal, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas

electrónicas de los delitos. En el mismo sentido, se deben tener presente los principios generales relativos a la asistencia mutua.

De igual manera, para poder establecer un procedimiento a utilizar para la investigación de los delitos relacionados a la Deep Web, es necesario adecuar la legislación interna y verificar los delitos contenidos en el Convenio de Budapest. Así pues, en dicho instrumento se prevén delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos (acceso ilícito, interceptación ilícita, interferencia en los datos, interferencia en el sistema y abuso de dispositivos); delitos informáticos propiamente (falsificación informática, fraude informativo); delitos relacionados con el contenido (pornografía infantil) y delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

4.2.- Recomendaciones

- Se recomienda al Estado venezolano suscribir y ratificar el Convenio sobre Cibercriminalidad de Budapest.
- Se recomienda al Estado venezolano reformar su Ley Especial sobre Delitos Informáticos para adecuarla a los hechos delictivos asociados a la Deep Weeb.
- Se recomienda a las instituciones especializadas en informática del país, dictar charlas, cursos, foros, entre otros encuentros académicos acerca de la noción, alcance e implicaciones de los delitos asociados a la Deep Web.
- Se recomienda a los docentes en la materia de Derecho Penal y Derecho Internacional abordar con mayor profundidad el tema de los delitos informáticos.
- Se recomienda a futuros investigadores desarrollar otros aspectos de esta temática, por cuanto se verificó en el marco de la investigación que no abundan los trabajos de grado relacionados con el contexto jurídico de la Deep Web.

BIBLIOGRAFÍAS

IMPRESAS

Alfonso, I. (1999). Técnicas de Investigación Bibliográfica. 8va. Edición. Contexto. Caracas, Venezuela.

Ander-Egg, E. (1988). Introducción a las técnicas de Investigación (19 ed.) Humanitas. Buenos Aires, Argentina.

Arias, F. (1998). El Proyecto de Investigación. Guía para su Elaboración. Editorial Episteme. Caracas - Venezuela.

Arias, F. (2004). El Proyecto de Investigación. Guía para su Elaboración. Editorial Episteme. Caracas - Venezuela.

Ávila, P. (2015). Diseño y evaluación de un taller de "seguridad en redes sociales" dirigido a los docentes de educación media general de informática (Trabajo de grado). Universidad Central de Venezuela.

Balestrini, M. (2002). Cómo se Elabora el Proyecto de Investigación. Sexta Edición. Editorial BL Consultores Asociados. Caracas - Venezuela.

Bautista, D. (2014). Deep Web: aproximaciones a la ciber irresponsabilidad. Revista Latinoamericana de Bioética, 15(1), 26-37.

Castells, M. (2001). La Galaxia Internet. Barcelona: Areté.

De la Corte, L., y Blanco, J (2014). Seguridad nacional, amenazas y respuestas. España: LID.

Hernández, L. (2009). El delito informático. Eguzkilore: Cuaderno del Instituto Vasco de Criminología. Nº 23.

Hernández, R.; Fernández, C. Y Batista, P. (2000). Metodología de la Investigación: Manual de Apoyo para Profesores. Editorial Mc- Graw Hill. México – Ciudad de México.

Jiménez, L. (1980). La Ley y el Delito. Buenos Aires, Argentina.

Jiménez, J. (2018). El contexto jurídico de la Deep Web (trabajo de grado) Universidad Rafael Landívar. Guatemala.

Loredo, J. y Ramírez, A. (2013). Delitos Informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. Facultad de Ciencias Físico Matemáticas. Universidad Autónoma de Nuevo León.

Moisés, B. A. (2018). Derecho público y propiedad intelectual: su protección en internet. Madrid: Editorial Reus.

Morales, R. y Alvarado, R. (2012). Cibercrimen. Guatemala: IUS Ediciones.

Ortiz, N. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. Revista Científica Hallazgos, 21(1), 100- 111.

Oxman, N. (2013). Estafas Informáticas a través de internet acerca de la imputación penal del "*phishing*" y el "*pharming*". Revista de derecho de la Pontificia Universidad Católica de Valparaíso, 262. Chile.

Ruiz, E. (2017). Nuevas tendencias en los sistemas de información. Buenos Aires: Editorial Centro de Estudios Ramon Areces SA.

Sabino, C. (2000). El Proceso de Investigación. Panapo. Caracas.

Tamayo, T. (1995). El Proyecto de Investigación. Editorial Grupo Noriega. Caracas, Venezuela.

Temperini, M. (2018). Delitos informáticos y cibercrimen: alcances, conceptos y características. Ciudad Autónoma de Buenos Aires: Erreius

Téllez, J. (1998). Derecho Informático. Editorial McGraw-Hill. México – Ciudad de México.

ELECTRÓNICA

Asamblea Nacional de Venezuela (2001). Ley Especial contra los Delitos Informáticos. Recuperado de: https://www.wipo.int/edocs/lexdocs/laws/es/ve/ve041es.pdf

Asociación de Internautas (2020). Deep Web: concepto, características y niveles. Recuperado de: www.internautas.org

BBC Mundo. (2017). Finanzas personales. Los 5 productos ilegales que más se venden en internet. Recuperado de: http://www.finanzaspersonales.co/consumointeligente/articulo/cosas-ilegales-en-internet/60740

Consejo de Europa (2001). Convenio Sobre la Ciberdelincuencia. Budapest.

Fernández, E. (2015). La Deep Web. Recuperado de: https://www.academia.edu/5145582/Trabajo_Deep_Web

Flores, L. (2014). Derecho Informático. México: Grupo Editorial Patria.

García, J. (2016). Cien horas en la Internet Profunda. Recuperado de: http://www.magazinedigital.net/historias/reportajes/cien-horas-eninternet-profunda

García, N. (2015). Cómo actuar si sufres calumnias e injurias en Internet. Recuperado de: https://www.kaspersky.es/blog/como-actuar-si-sufres-calumnias-e-injurias-eninternet/6150/

González, C. (2015). Por qué Tor funciona lento, y como se puede navegar más rápido por la Deep Web. Recuperado de: https://www.adslzone.net/2015/09/23/por-que-tor-funciona-lento-y-como-se-puedenavegar-mas-rapido-por-la-deep-web/

Iglesis, C. (2018). La criminalidad en internet. Recuperado de: http://www.abacus.universidadeuropea.es/bitstream/handle/11268/4954/Iglesias_Carballo_ 2001.pdf?sequence=1

Oficina de las Naciones Unidas contra la Droga y el Delito. (2013). El uso del internet con fines terroristas. Recuperado de https://www.unodc.org/...Internet.../Use_of_Internet_Ebook_SPANISH_for_web.pdf

Organización Mundial de la Propiedad Intelectual. (2018). La OMPI por dentro. Recuperado de: http://www.wipo.int/about-wipo/es/

Tecnoxplora. (2015). El 80% de lo que circula por la internet profunda es pornografía infantil. Recuperado de: https://www.lasexta.com/tecnologia-tecnoxplora/internet/quecircula-internet-profunda-pornografiainfantil_2015011257f78f110cf2fd8cc6aa9ddf.html