UNIVERSIDAD RAFAEL LANDÍVAR
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
LICENCIATURA EN CIENCIAS JURÍDICAS Y SOCIALES

"EL CONTEXTO JURÍDICO DE LA DEEP WEB"

TESIS DE GRADO

JOSÉ ANDRES JIMÉNEZ ROSALES
CARNET 10234-12

GUATEMALA DE LA ASUNCIÓN, OCTUBRE DE 2018
CAMPUS CENTRAL

UNIVERSIDAD RAFAEL LANDÍVAR
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
LICENCIATURA EN CIENCIAS JURÍDICAS Y SOCIALES

"EL CONTEXTO JURÍDICO DE LA DEEP WEB"

TESIS DE GRADO

TRABAJO PRESENTADO AL CONSEJO DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

POR
JOSÉ ANDRES JIMÉNEZ ROSALES

PREVIO A CONFERÍRSELE

EL GRADO ACADÉMICO DE LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

GUATEMALA DE LA ASUNCIÓN, OCTUBRE DE 2018
CAMPUS CENTRAL

AUTORIDADES DE LA UNIVERSIDAD RAFAEL LANDÍVAR

RECTOR:	P. MARCO TULIO MARTINEZ SALAZAR, S. J.
VICERRECTORA ACADÉMICA:	DRA. MARTA LUCRECIA MÉNDEZ GONZÁLEZ DE PENEDO
VICERRECTOR DE INVESTIGACIÓN Y PROYECCIÓN:	ING. JOSÉ JUVENTINO GÁLVEZ RUANO
VICERRECTOR DE INTEGRACIÓN UNIVERSITARIA:	P. JULIO ENRIQUE MOREIRA CHAVARRÍA, S. J.
VICERRECTOR ADMINISTRATIVO:	LIC. ARIEL RIVERA IRÍAS
SECRETARIA GENERAL:	LIC. FABIOLA DE LA LUZ PADILLA BELTRANENA DE LORENZANA

AUTORIDADES DE LA FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

DECANO:	DR. ROLANDO ESCOBAR MENALDO
VICEDECANA:	MGTR. HELENA CAROLINA MACHADO CARBALLO
SECRETARIO:	LIC. CHRISTIAN ROBERTO VILLATORO MARTÍNEZ
DIRECTOR DE CARRERA:	MGTR. ALAN ALFREDO GONZÁLEZ DE LEÓN
DIRECTOR DE CARRERA:	MGTR. JUAN FRANCISCO GOLOM NOVA
DIRECTORA DE CARRERA:	MGTR. ANA BELEN PUERTAS CORRO

NOMBRE DEL ASESOR DE TRABAJO DE GRADUACIÓN

LIC. ANDY GUILLERMO DE JESUS JAVALOIS CRUZ

TERNA QUE PRACTICÓ LA EVALUACIÓN

MGTR. HELENA CAROLINA MACHADO CARBALLO

Ciudad de Guatemala, 27 de noviembre de 2017

Honorable
CONSEJO DE LA FACULTAD
DE CIENCIAS JURÍDICAS Y SOCIALES
DE LA UNIVERSIDAD RAFAEL LANDÍVAR
Presente.

Tengo el agrado de dirigirme a Ustedes en relación a la asesoría en la investigación del trabajo de Tesis del estudiante **JOSÉ ANDRES JIMÉNEZ ROSALES** con carné número 1023412 previo a optar el grado académico de **LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES** y los títulos de **ABOGADO Y NOTARIO.**

La investigación realizada por el estudiante se titula ***"El Contexto Jurídico de la Deep Web";*** misma que a juicio del suscrito reúne los requisitos metodológicos y sustantivos de la Universidad Rafael Landívar y constituye un aporte importante.

Hago de su conocimiento de honorable Consejo de Facultad que durante el tiempo que me desempeñe como asesor del estudiante pude confirmar dedicación y diligencia aplicada para desarrollar su investigación.

En virtud de lo anterior, por medio de la presente y en cumplimiento del encargo del Consejo de la Facultad, tengo el gusto de emitir **DICTAMEN FAVORABLE** a la tesis de **JOSÉ ANDRES JIMÉNEZ ROSALES.**

Sin otro particular me suscribo de ustedes.

Atentamente:

Lic. Andy Guillermo Javalois Cruz

Omnia Ad Maiorem Dei Gloriam
Arq. Guillermo de Jesus Javalois Cruz
Abogado y Notario

Licda. Helena C. Machado
Abogada y Notaria

Guatemala, 07 Marzo 2018.

Señores
Miembros del Consejo
Facultad de Ciencias Jurídicas y Sociales
Universidad Rafael Landívar
Ciudad

Honorables Miembros del Consejo:

Me dirijo a ustedes con el objeto de hacer de su conocimiento que, en cumplimiento al nombramiento recaído en mi persona, procedí a realizar la ***Revisión de Fondo y de Forma*** a que se refiere el Instructivo de Tesis de la Facultad de Ciencias Jurídicas y Sociales, del trabajo de tesis titulado **"EL CONTEXTO JURÍDICO DE LA DEEP WEB"** elaborado por el estudiante **JOSÉ ANDRÉS JIMÉNEZ ROSALES.**

Luego de efectuada la revisión, se sugirieron varias correcciones al autor de la Tesis, quien cumplió con presentar las mismas dentro del plazo establecido en el Instructivo de Tesis de esa Facultad. En tal virtud, considero que el contenido de la tesis en referencia se encuentra estructurado conforme a los requerimientos y regulaciones existentes de la Universidad Rafael Landívar para el efecto.

Por lo expuesto, emito a favor del trabajo de tesis investigado y elaborado por José Andrés Jiménez Rosales de conformidad con los requisitos reglamentarios, **DICTAMEN FAVORABLE SOBRE LA PERTINENCIA DE EMITIR LA ORDEN DE IMPRESIÓN**, a efecto de que se continúen con los procedimientos establecidos por esa Universidad, toda vez que el presente trabajo es apto como tesis para que al autor del mismo se le confiera el Grado Académico de Licenciado en Ciencias Jurídicas y Sociales.

Habiendo cumplido con el encargo encomendado por esa Facultad, me suscribo con muestras de mi consideración y respeto.

Atentamente,

Mgtr. Helena Carolina Machado Carballo

11 calle 22-49 zona 11 Residenciales San Jorge, Guatemala, Guatemala
Teléfono: (502) 52067861
E-mail: machadohc@gmail.com

Universidad Rafael Landívar
Tradición Jesuita en Guatemala

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
No. 071722-2018

Orden de Impresión

De acuerdo a la aprobación de la Evaluación del Trabajo de Graduación en la variante Tesis de Grado del estudiante JOSÉ ANDRES JIMÉNEZ ROSALES, Carnet 10234-12 en la carrera LICENCIATURA EN CIENCIAS JURÍDICAS Y SOCIALES, del Campus Central, que consta en el Acta No. 0789-2018 de fecha 7 de marzo de 2018, se autoriza la impresión digital del trabajo titulado:

"EL CONTEXTO JURÍDICO DE LA DEEP WEB"

Previo a conferírsele el grado académico de LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES.

Dado en la ciudad de Guatemala de la Asunción, a los 29 días del mes de octubre del año 2018.

LIC. CHRISTIAN ROBERTO VILLATORO MARTÍNEZ, SECRETARIO
CIENCIAS JURÍDICAS Y SOCIALES
Universidad Rafael Landívar

AGRADECIMIENTOS

A Dios, por darme la vida, mi familia, mi hogar, por su amor incondicional, por estar siempre a mi lado ante las pruebas difíciles, escuchar mis oraciones y por darme las oportunidades para seguir mis sueños y anhelos.

A mis papás, *Juan José Jiménez Soto y Leslie Damaris Rosales de Jiménez,* por el amor que me han demostrado siempre, por los buenos valores que me han inculcado, por darme educación, por haberme inspirado para seguir esta carrera universitaria, por el apoyo que nunca me han negado y por demostrarme que con esfuerzo y dedicación las metas pueden ser alcanzadas.

A mis hermanos, *Diego Estuardo y Leslie Eunice,* por traer muchas alegrías a mi vida y ser mis fieles compañeros a lo largo de los años.

A mis abuelos, *José Isidro Jiménez y Ana Orfina de Jiménez,* a quienes especialmente dedico este trabajo, por el amor y apoyo que me han dado a lo largo de los años y por creer siempre en mí.

A mi familia, por alentarme en todo momento, estar pendiente de mis pasos y brindarme su apoyo siempre.

A mis colegas, por haber compartido conmigo muchas experiencias a lo largo de mi vida universitaria y quienes siempre me han demostrado su lealtad y compañerismo.

A mis amigos, quienes me han demostrado su cariño y apoyo en todo momento, quienes me han ayudado a acercarme más a Dios y en quienes puedo confiar grandemente.

1 Timoteo 4:12

Responsabilidad: El autor es el único responsable de los contenidos y conclusiones de la presente tesis.

LISTADO DE SIGLAS Y ABREVIATURAS

CIA:	Central Intelligence Agency (Agencia Central de Inteligencia)
CSIRT:	Computer Security Incident Response Team (Equipo de Respuesta a Incidentes de Seguridad Informática)
FBI:	Federal Buro of Investigation (Buró Federal de Investigaciones)
INACIF:	Instituto Nacional de Ciencias Forenses de Guatemala
INTERPOL:	International Criminal Police Organization (Organización Internacional de Policía Criminal)
MP:	Ministerio Público
NSA:	National Segurity Agency (Agencia de Seguridad Nacional)
PCN:	Procuraduría General de la Nación

RESUMEN EJECUTIVO

La presente investigación aborda la temática de la *Deep Web o Internet Profunda*, el impacto que ha generado en general a nivel mundial y en particular en el medio guatemalteco, confrontándola con la normatividad vigente. De esa cuenta, la investigación realizada ha girado en torno a la siguiente interrogante: ¿Cuál es el contexto jurídico pertinente para la Deep Web?

El trabajo se encuentra dividido en seis capítulos siendo los primeros cinco los destinados a desarrollar elementos necesarios para la comprensión y análisis de conceptos relacionados con la Deep Web y su conceptualización jurídica tales como: Concepto de la Deep Web o Internet Profunda, características de la Internet Profunda, peligros y amenazas, actividad ilícita, delitos informáticos, bienes jurídicos tutelados, sujeto activo, sujeto pasivo, clasificaciones, vulnerabilidad del patrimonio y propiedad intelectual, violación a la privacidad, la intimidad, libertad e indemnidad sexual, cooperación penal internacional, convenios internacionales, entidades e instituciones que velan por la seguridad informática, territorialidad y alcance de la ley penal, legislación nacional e internacional en materia, protección jurídica de los programas de computación y ordenadores y descripción de casos relacionados en la vida real.

En el sexto capítulo se realiza la presentación, análisis y discusión de resultados con fundamento en las entrevistas, en confrontación con el marco teórico, utilizadas para establecer las conclusiones y recomendaciones de la presente investigación y alcanzar los objetivos trazados en la misma.

INDICE

INTRODUCCION……1

CAPÍTULO 1: La *Deep Web o* Internet Profunda……4

1.1. Concepto de la Deep Web o Internet Profunda……4

1.2. Características de la Internet Profunda……8

1.2.1. Tamaño……9

1.2.1.a Niveles de la Internet Profunda……11

1.2.2. Acceso……12

1.2.2.a. Tor (The Onion Router) o El Enrutador Cebolla……14

1.3. Peligros y Amenazas……15

1.3.1. Actividad Ilícita en la Internet Profunda……16

1.3.2. La Darknet o Dark Web……17

1.3.2.a. Bitcoin……18

CAPÍTULO 2: Los Delitos Informáticos……20

2.1. Concepto de Delitos Informáticos……20

2.2. Origen del Delito Informático……24

2.3. Bien Jurídico Tutelado……26

2.4. Sujeto Activo……29

2.5. Sujeto Pasivo……30

2.6. Clasificaciones del Delito Informático……31

2.6.1. Delitos Informáticos contra el Patrimonio y la Propiedad Intelectual……32

2.6.2. Delitos Informáticos que atentan contra la Privacidad, la intimidad, la Libertad o Indemnidad Sexual…… 33

CAPÍTULO 3: Legislación……34

3.1. La Cooperación Penal Internacional……35

3.2. Convenios Internacionales……37

3.2.1. Convenio de Budapest……37

3.2.2. Convenio No. 108 del Consejo de Europa de 28 de enero de 1981, para la protección de las personas con respecto tratamiento automatizado de datos de carácter personal.....39
3.2.3. Decisión Marco 2005/222/JAI.....40
3.3. La Organización de las Naciones Unidas y la Prevención del Delito Informático 40
3.3.1. Declaración de Viena sobre la Delincuencia y la Justicia frente a los retos del siglo XXI 41
3.3.2. Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos.....42
3.3.3. Tratado de la Organización Mundial de la Propiedad Intelectual sobre el Derecho de Autor.....42
3.4. Territorialidad y Alcance de la Ley Penal.....43
3.5. Legislación Guatemalteca.....44
3.5.1. Iniciativa de Ley No. 4055 Ley de Delitos Informáticos.....46
3.5.2. Iniciativa de Ley No. 5254 Ley contra la Ciberdelincuencia.....48
3.6. Derecho Comparado.....49
3.6.1. España.....49
3.6.2. Estados Unidos.....50
3.6.3. Argentina.....51
3.6.4. Colombia.....51
3.6.5. México.....52
CAPÍTULO 4: Análisis de Normatividad Guatemalteca Específica hacia el Derecho Convencional.....53
4.1. Normativa Nacional.....53
4.1.1. Violación a Derechos de Autor contenida en el artículo 274 del Código Penal.....57
4.1.2. Violación a los Derechos de Propiedad Industrial contenida en el artículo 275 del Código Penal.....59
4.1.3. Violación a la intimidad sexual contenida en el artículo 190 del Código Penal.....60

4.1.4. Producción de pornografía de personas menores de edad contenida en el artículo 194 del Código Penal; y la Comercialización o difusión de pornografía de personas menores de edad contenida en el artículo 195 Bis.....62
4.1.5. Comercialización de Datos Personales ilícito penal contenido en la Ley de Acceso a la Información Pública, artículo 64.....63
4.2. Protección Jurídica Informática en el Derecho Convencional.....64
4.2.1. Protección Jurídica de los Datos Personales e Intimidad Personal de los usuarios de Internet.....67
4.2.2. Protección Jurídica de los programas de computación y ordenadores.....69
CAPÍTULO 5: Casos relacionados a la Internet Profunda y Delitos Informáticos 71
5.1. Silk Road 71
5.2. Wikileaks.....75
5.3. Anonymous.....78
CAPÍTULO 6: Presentación, Análisis y Discusión de Resultados.....81
6.1 Entrevistas.....82
6.1.1 Primer Modelo de Entrevista.....82
6.1.2 Segundo Modelo de Entrevista……..90
6.2 Discusión y Análisis de Resultados.....92
CONCLUSIONES.....96
RECOMENDACIONES.....97
LISTADO DE REFERENCIAS.....98
ANEXOS.....107

INTRODUCCIÓN

Internet es la tecnología más importante de la sociedad de la información ya que es el motor de las comunicaciones y las redes informáticas, lo cual proporciona una posibilidad ilimitada de una comunicación interactiva en cualquier momento y con libertad de desarrollo, lo cual permite la creación de contenido que no es indexado por lo motores de búsqueda convencionales surgiendo a partir de ello un sitio, anónimo y virtualmente indetectable, conocido como Deep Web o Internet Profunda, ésta permite el acceso a una amplia gama de información que deviene de la libertad que ofrece a los usuarios, quienes se valen de nuevas herramientas informáticas que facilitan el ejercicio de sus actividades.

El desarrollo del objeto material tiene por finalidad demostrar que puede dársele una descripción jurídica al entorno de la Deep Web, lo que denota que todo ese vasto objeto de estudio conduce a la verificación de dicho planteamiento, que al comprobarse tendrá implicaciones de carácter teórico y práctico, porque a su vez resaltará la importancia de utilizarla para la comprensión y análisis de las repercusiones en los distintos sectores en cuanto a las irregularidades en la actividad informática. Por tal razón, el aporte de esta investigación está integrado por su objeto de estudio, su enfoque y verificación de objetivos. En efecto, es una contribución el estudio sistemático, claro y concreto de la Deep Web en general, y evidenciar las relaciones, imprecisiones y limitaciones entre los usuarios afectos a su uso con énfasis en las consecuencias de carácter jurídico en las que éstas pueden implicar.

El contenido de la investigación está expuesto de forma adecuada y precisa lo cual le da al trabajo un aporte teórico valioso que tendrá consecuencias en el aspecto práctico, de tal manera que busca: a) Definir el término Deep Web o Internet Profunda, así como sus características y funcionamiento en la red; b) describir los principios y normas que regulan los efectos jurídicos de la relación entre el Derecho y la Informática; c) explicar cómo la Internet Profunda en los últimos años ha llegado

a ser un tema de controversia a nivel mundial; d) analizar la protección jurídica aplicable a los usuarios de Internet a partir de la regulación normativa surgida de tratados internacionales; e) clasificar y describir el tipo de actividades realizables en la plataforma “Deep Web” a partir de la amplia brecha digital que proporciona**;** f) describir los derechos que pueden ser vulnerados o protegidos en su utilización; y, g) analizar el impacto que genera en la sociedad virtual la existencia de las facilidades que la Deep Web proporciona a partir del anonimato y los casos reales que han surgido por el uso irresponsable que se le ha dado a la plataforma.

No existieron límites en cuanto al costo y disponibilidad para el desarrollo de la investigación porque se tuvo acceso a gran número de fuentes pertinentes. Ahora bien, entre los límites que se presentaron están: Los precisados por el mismo objeto de estudio y la falta de conocimiento de algunos profesionales respecto a la temática de la investigación, en virtud de ello se utiliza como instrumento para recabar y sistematizar la información de la investigación la entrevista permitiendo de esta forma la obtención de información objetiva basada en una guía de preguntas con carácter general y particular, para abarcar tanto aspectos teóricos como prácticos.

La presente investigación es una monografía de tipo jurídico descriptiva empleándose para el efecto la metodología descriptiva, porque se puntualizaron y explicaron los elementos acerca de la Deep Web, así como sus teorías más representativas y sus relaciones.

Para los efectos de la realización de esta monografía se siguieron los siguientes pasos lógicos: Recopilación y estudio de más información bibliográfica pertinente, desarrollar ordenadamente, y por capítulos, los antecedentes del tema y el marco teórico, conforme al índice esquemático del anteproyecto, realización de las entrevistas estructuradas dirigidas a los sujetos de estudio, análisis y redacción de los resultados de los instrumentos utilizados, con su respectiva interpretación y confrontación con los antecedentes y marco teórico del trabajo, determinando si se alcanzaron los objetivos trazados y si se respondió a la pregunta de investigación:

¿Cuál es el contexto jurídico pertinente para la Deep Web? Además, el desarrollo claro, breve y preciso de las conclusiones del trabajo, así como de las recomendaciones pertinentes.

CAPÍTULO 1

La *Deep Web* o *Internet Profunda*

1.1 Concepto de la *Deep Web o Internet Profunda*

El autor Pedro Alberto De Miguel Asensio, identifica a la Internet como «*un elemento clave de la llamada sociedad de la información, pues facilita los más variados servicios electrónicos interactivos y la comunicación de todo tipo de informaciones*»[1] entre ellos: textos, sonidos, imágenes, vídeos, etc. Esto la constituye como un entramado de redes conectadas entre sí de un modo que hace posible la comunicación desde cualquier ordenador convirtiéndola en un medio global para el desarrollo de informaciones.

La Real Academia Española, citada por Mariliana Rico Castillo, define al ciberespacio como un ámbito artificial creado por medios informáticos; de esta manera, reconociendo un concepto que el novelista William Gibson desarrolló en su obra *«Neuroamanecer»* para referirse a una alucinación mediante la cual se podía sentir real un espacio generado computacionalmente, sin contar con un correlato en el mundo físico.[2] La autora refiere además que, en cada uno de los ciberespacios que se forman en torno a todos los usuarios de Internet es posible encontrar una extensión de la vida, con una multiplicidad de problemas políticos, económicos, sociales y éticos que exigen una valoración constante.[3]

Rolando Alvarado y Ronald Morales, por su parte, definen al Internet como «*una red informática mundial que se utiliza como un «medio de comunicación», formada por la conexión directa entre computadoras u ordenadores, mediante un protocolo especial de comunicación.»*[4] Esto da a entender la existencia de una brecha que

[1] De Miguel Asensio, Pedro Alberto. *Derecho Privado de Internet.* España. Editorial Civitas. 2015. 3ra. Edición. Pág. 27
[2] Rico Carrillo, Mariliana. *Derecho de las nuevas tecnologías.* Argentina. Ediciones La Rocca. 2007. Página 51
[3] Loc. Cit.
[4] Morales, Ronald y Rolando Alvarado. *Cibercrimen*. Guatemala. IUS Ediciones. 2012. Pág.10

permite la creación de las fuentes de información en la plataforma de la Internet que se encuentra vulnerable a la intervención de distintos usuarios cuyos fines tienen diferente enfoque que en ocasiones atentan al bien común.

Alvarado y Morales también definen a la Internet como un conjunto descentralizado de redes de comunicación interconectadas, que utilizan el protocolo de control de transporte y el protocolo de Internet, según sus siglas en inglés: TCP/IP; garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. [5]

De Miguel Asensio señala que, por su carácter descentralizado, no es posible que un organismo dirija y gestione Internet. Su funcionamiento es consecuencia del empleo, por una gran cantidad de operadores de sistemas informáticos y de redes, de protocolos comunes.[6] Esto significa que se permite un intercambio con total exactitud de información digital que abre la brecha hacia una cantidad infinita de datos y contenido de distinto tipo y fin, tomando en cuenta que la red proporciona muchas facilidades para compartir y generar nuevos contenidos.

De acuerdo con Lucerito Flores Salgado, dentro del entorno jurídico de las telecomunicaciones y la informática en el que actualmente se encuentran los seres humanos, se han tratado sobre temas que implican el uso de la computadora. Se puede intentar dar respuesta a cada problema que surja regulando situaciones, como contratos electrónicos, delitos en este medio, valor probatorio de los documentos electromagnéticos, internet, comercio electrónico, firmas digitales, datos personales, contenidos en las bases de datos o la llamada piratería. Sin embargo, no se hace un análisis del por qué hablar de estos problemas, sino que se hace un enfoque sobre: de dónde surgen, por qué hablar de derecho e informática.[7]

---

[5] Ibíd. Página 10
[6] De Miguel Asensio, Pedro Alberto de. *Op. Cit.* Pág. 28
[7] Flores Salgado, Lucerito. *Derecho Informático.* México. Laurousse – Grupo Editorial Patria. 2014. Página 4

En relación a la eficacia del Derecho en el ciberespacio, de acuerdo con Rico Castillo, los argumentos sobre la anarquía de la red suelen ser frecuentes. En efecto, si se considera a la anarquía como la ausencia del poder coercitivo del Estado; lo cual hace estar frente a un deseo de libertad que recobra fuerza en el plano de gobernabilidad, sobre todo si la Internet se presenta como un medio de comunicación que no es necesariamente capaz de resolver cabalmente la crisis de representatividad por la cual atraviesan las democracias.[8]

Además, como lo expresa Rico Castillo, los poderes públicos experimentan de esta forma problemas para gobernar con eficacia en Internet, viendo debilitada su soberanía por el fenómeno de globalización en los medios y la comunicación electrónica, en delincuencia y en las actividades económicas, ya que debido a la internacionalización, la Internet puede ser calificada como políticamente subversiva, desde el momento en que debilita el poder del Estado mediante la creación de ámbitos de actividad alternativos a él, que cambian las relaciones internacionales dentro del ciberespacio, a través del reemplazo de los tradicionales sujetos estatales por la sociedad civil organizada en torno a comunidades virtuales.[9]

La denominada *Deep Web* o *Internet Profunda* que en la obra «*The Deep Web: Surfacing Hidden Value»,* del autor Michael Bergman, se compara con el acto de buscar información en la red con la pesca en el gran océano, en cuya superficie puede encontrarse mucha información, con el problema de existir cierta cantidad de difícil acceso, y, por lo tanto, oculta.[10] Previamente, en 1994, la doctora Jill Ellsworth, especializada en el estudio de la Red, citada por Idioa Salazar García, acuñó el término «*Internet invisible»* para referirse a la información que no podían encontrar

[8] Rico Castillo, Mariliana. *Óp. Cit.* Página 52
[9] Ibid. Página 53
[10] Semantic Scholar. Bergman, Michael K. *The Deep Web: Surfacing Hidden Value.* Estados Unidos. 2000. Disponible en: https://www.semanticscholar.org/paper/The-Deep-Web-Surfacing-Hidden-Value-BERGMAN/0a59b63213f26b4e695ee01065163ba1769cf861 Fecha de consulta: 26/02/2017

los buscadores más comunes por razones técnicas o simplemente por conveniencia.[11]

Según Carlos González, en un sentido más amplio, la Internet está ideada para la *indexación* de contenidos, ya que no es más que una red de ordenadores y dispositivos conectados, siendo algunos los que juegan el papel de *servir información*. Estos servidores son los que almacenan la información de las páginas web que sirven y, entre los ficheros de estas páginas web, se encuentran algunos configurados para ser leídos por los buscadores comunes como *Google, Microsoft, Yahoo* y otras compañías que revisan este fichero, lo interpretan y generan un "índice" de su contenido, de tal manera que sea sencillo encontrar contenido del interés del usuario.[12]

De acuerdo con De Miguel Asensio, *(…) la comunicación entre los ordenadores conectados a Internet es posible en la medida en que cada uno de ellos está plenamente identificado (…).*[13] De acuerdo a lo anterior, para el acceso al contenido de una página web se necesita de un dominio que sirva como puerta de acceso hacia los archivos de la página web de interés del usuario. Analizando a lo señalado por González, se puede catalogar que la *Deep Web* está configurada de tal manera que los motores de búsqueda no pueden indexar la información de las páginas web, o, en otras palabras, no es posible el acceso a este contenido a través de estos buscadores.

Entre los antecedentes de la temática a tratar se hace énfasis en que la mayor parte de los internautas tienen necesidades que resuelven en la red a la manera de investigación, comunicación, consumo y entretenimiento. Para el autor Nathan

---

[11] Observatorio Para la Cibersociedad. Salazar García, Idoia. *La Red Profunda. Lo que los buscadores convencionales no encuentran.* España. 2004. Disponible en: http://www.cibersociedad.net/congreso/comms/g20salazar.htm Fecha de Consulta: 25/02/2017

[12] ADSL ZONE. González, Carlos. *La Deep Web no es un lugar para impulsivos, morbosos e inexpertos.* España. 2015. Disponible en: https://www.adslzone.net/2015/06/14/la-deep-web-no-es-lugar-para-impulsivos-morbosos-e-inexpertos/ Fecha de Consulta: 25/02/2017

[13] De Miguel Asensio, Pedro Alberto de. *Óp. Cit.* Página 43

Chandler, es así como la búsqueda de información en general, correo electrónico, la compraventa de productos, redes sociales y el acceso a cualquier tipo de entretenimiento se constituyen como los motivadores principales del acceso a internet y, en consecuencia, del trabajo de los motores de búsqueda ofrecen millones de resultados inmediatos y, en general, muy útiles.[14]

Sin embargo, estos resultados tienen entre sus desventajas la falta de confiabilidad y calidad que estos pueden proporcionar dependiendo de las necesidades que tenga el internauta. Esto es así porque lo que se puede percibir con el uso simple de los motores de búsquedas es apenas la superficie de un gran campo informático, causando de esta forma la existencia de una plataforma capaz de albergar cantidades mayores de contenido que no poseen una facilidad de acceso simple.

Según Edna Martínez, los principios y normas que conforman el derecho informático son indispensables en el análisis de la plataforma virtual a estudiar, puesto que de ella es posible el desarrollo e implementación de sistemas informáticos, sistematización de procesos, facilitación del acceso de datos de diferentes contenidos, los cuales son objeto de estudio por sus implicaciones legales que pueden surgir.[15]

1.2. Características de la Internet Profunda

Para el estudio de la plataforma Internet Profunda, a continuación, se hace un desarrollo de las características con las que cuenta.

---

[14] Biblioteca Pleyades. Chandler, Nathan. *Cómo funciona la Internet Profunda*. Estados Unidos. 2015. Disponible en: http://www.bibliotecapleyades.net/sociopolitica/sociopol_internet214.htm Fecha de consulta: 24/01/2017

[15] Martínez Solórzano, Edna Rossana. *Apuntes de Derecho Informático.* Guatemala. Ediciones Mayte. 2012. Página. 7

1.2.1 Tamaño

Existe una comparación muy ilustrativa en la que se compara la Internet con un iceberg. David Tabóas menciona, acerca de la dimensión que tiene esta plataforma, que se podría representar la profundidad mediante esta figura, en donde la parte superficial o la punta del iceberg correspondería a un veinticinco por ciento (25%) de su proporción, o sea, entra aquí el contenido regulado por los buscadores estandarizados comunes los cuales están familiarizados con la mayor parte de los usuarios de Internet. Por otro lado, la parte sumergida del iceberg, sería proporcional a la *Internet Profunda o Deep Web,* correspondiendo a un setenta y cinco por ciento (75%) en donde se encuentra casi la totalidad de la información que puede proporcionar la red.[16]

Los argumentos de Tabóas, acerca de la dimensión de la *Internet Profunda* brindan un aporte acerca del concepto sobre cómo debe entenderse la parte superficial de la Internet, aunque pareciera un campo bastante amplio en cuanto contenido e información, no sería más que una pequeña parte que conforma la totalidad de la plataforma que consiste en la red. El resto consistiría en todo aquel contenido, que, en párrafos anteriores, se denomina como *Deep Web o Internet Profunda*. Además, la metáfora del iceberg para comprender el término, se vale también para entender su tamaño en donde la parte más grande de Internet es la que no tiene fácil acceso.

Al ser un área tan vasta en cuanto contenido, es menester hacer mención sobre el tamaño que ésta posee. Para medirla se debe hacer por medio de la unidad universal de información denominada como *byte.* Jorge A. González lo define como «*una agrupación de ocho bits que permite cifrar y representar un signo o carácter»*[17]*.* Esto quiere decir que por medio de esta unidad llega a existir la capacidad para contener la información digita encontrada en la red.

---

[16] Universitat Oberta de Catalunya. Tabóas, David. *¿Qué esconde la Deep Web?* España. 2016. Disponible en: https://www.uoc.edu/portal/es/uoc-news/actualitat/2016/043-deep-web.html Fecha de Consulta: 24/02/2017

[17] González, Jorge A. y otros. *Cibercultura e iniciación en la investigación.* México. Colección Intersecciones. 2007. Pág. 121

Aunado a esto, De Miguel Asensio argumenta que «l*a comunicación entre los ordenadores conectados a Internet es posible en la medida en que cada uno de ellos está plenamente identificado. El elemento que hace posible esa identificación es la dirección IP (Internet Protocolo), que consiste en una dirección numérica, basada tradicionalmente en números de treinta y dos (32) bits de longitud.»*[18] Adicionalmente, el autor señala que siendo estos dominios la venta de acceso hacia los contenidos en la red virtual para todos los usuarios de Internet, estos al no estar indexados por los motores de búsqueda genera la incapacidad de ingresar a contenido clasificado y privado. El sistema de nombres de dominio responde a una estructura jerárquica, tanto en el plano administrativo como técnico.[19]

Según un estudio de la Universidad de California de Berkeley, citado por Eliana Álvarez, estimó que la Internet Profunda tiene un tamaño de noventa y un mil *Terabytes* (91,000 TB).[20] Con esta estimación se puede tener una idea sobre la capacidad de almacenamiento que ha sido posible albergar en esa plataforma; según González, un *Terabyte* equivaldría a 50,000 árboles hechos de papel e impresos; 2 *terabytes* a una biblioteca de investigación académica; 10 *terabytes* a las colecciones impresas de la biblioteca del Congreso de Estados Unidos; y, 400 *terabytes* a la base de datos del Centro Nacional de Datos Climatológicos de Estados Unidos. [21]

Basado en la analogía anterior, se puede ilustrar a grandes rasgos la manera en la cual se encuentra conformada la Internet Profunda; sin embargo, a través de ello, debe recalcarse la distinción que se realiza al mencionar que es una estimación sobre esta plataforma, debido a que a su capacidad de almacenamiento no podría limitarse por su constante crecimiento digital puesto a la creación de nuevos

[18] De Miguel Asensio, Pedro Alberto. *Op. Cit.* Pág. 43
[19] Loc. Cit.
[20] Colombia Digital. Àlvarez, Eliana. *Internet Profunda: concepto, características y niveles.* Colombia. 2014. Disponible en: https://colombiadigital.net/actualidad/noticias/item/6558-internet-profunda-concepto-caracteristicas-y-niveles.html Fecha de consulta: 24/02/2017
[21] González, Jorge A. y otros. *Óp. Cit.* Pág. 40

contenidos que llegan a formar parte de sus unidades de información. Además, debe tomarse en cuenta que no sería imposible que con el transcurso de los años y las facilidades de acceso virtual la Internet Profunda tenga un mayor crecimiento.

De acuerdo con lo establecido por González, respecto a la indexación de contenidos, se puede argumentar que la Internet Profunda como tal, trata aquella información que está disponible en Internet pero que únicamente es accesible a través de páginas generadas dinámicamente tras realizar una consulta en una base de datos. Analizando ello, puede señalarse, además, que esta plataforma es inaccesible mediante los procesos habituales de recuperación de la información tomando en cuenta que los servidores que se encuentran en este espacio son totalmente inaccesibles desde cualquier ordenador sin los procedimientos adecuados.

Por otro lado, a lo que se le definiría como la causa principal de la existencia de la Internet Profunda es la incapacidad de los motores de búsqueda comunes para acceder a la información existente en Internet, ya que si éstos tuvieran la capacidad para ingresar a esa información significaría la reducción casi en su totalidad de esta plataforma; aunque, no completamente por la existencia de páginas privadas que cuentan con un acceso generado a partir de contraseñas o códigos especiales.

1.2.1a Niveles de la Internet Profunda

La *Deep Web* por su amplio espacio en plataforma virtual se le ha dividido varios niveles, que son definidos por Miguel Ramos López-Quesada de la siguiente forma:

1. *Surface* o superficial: De acuerdo con Ramos López-Quesada, es el que los usuarios de Internet utilizan día a día. Se caracteriza por su censura hacia contenido peligroso y ofensivo de contenido ilegal es perseguido y eliminado. [22]

[22] Universidad CEU San Pablo. Miguel Ramos López-Quesada. *Deep Web*. España. 2015. Disponible en: http://informaticaemprendimiento.org/wp-content/uploads/2015/05/ramos-DEEP-WEB-1.pdf Página 2. Fecha de consulta: 21/02/2017

2. *Bergie*: Ramos López-Quesada señala que se refiere a aquellos sitios web donde los contenidos no tienen tanta censura aunque en ocasiones rozan la ilegalidad.[23]

3. *Deep*: Ramos López-Quesada manifiesta que este es el primer nivel que requiere cierta seguridad (con un proxy nos serviría para navegar relativamente de forma segura). El contenido es peligroso y a veces difícil de soportar.[24]

4. *Charter:* Según lo expresa Ramos López-Quesada, se necesita *TOR* para poder navegar en él. El contenido en este nivel de la Deep Web es realmente fuerte: libros y películas "baneadas", asesinos a sueldo, comercio de animales exóticos, contrabando, drogas, etc. Es también conocido como la *Darknet o Dark Web,* término que será desarrollado más adelante.[25]

5. Marianas: Conforme lo distingue Ramos López-Quesada, su nombre se debe a las fosas marianas, indicando que es un nivel muy profundo de internet. El contenido que ofrece este nivel de la *Deep Web* es incierto. Sólo se conoce sobre este nivel lo que los usuarios que han navegado por las marianas han revelado o compartido en la web convencional.[26]

1.2.2. Acceso

Según lo relacionado por los autores citados en el apartado anterior, existe una dificultad distintiva para tener acceso a la *Internet Profunda* puesto que en su contenido cuenta con zonas restringidas a los usuarios. Esto forma bases de datos de diferentes sitios web con gran cantidad de contenidos a los que no se puede

[23] Loc. Cit.
[24] Loc. Cit.
[25] Loc. Cit.
[26] Loc. Cit.

llegar a través de los buscadores convencionales. Esto da a entender que para el acceso a ello deben existir mecanismos especiales que proporcionen la facilidad hacia su navegación.

Fabricio Piciarelli señala que no todo lo que hay en el *deep web* es ilegal, ya que pueden encontrarse archivos y documentación comunes, por ejemplo de tipo médico, científico, académico o financiero que por motivos técnicos o de otra naturaleza no son accesibles a través de los normales motores de búsqueda. Aun así, el hecho de que sea posible una navegación en completo anonimato, fuera del alcance de policía y gobiernos, hace posible y fecundo el proliferar de actividades ilícitas de distinto tipo: páginas web pedo-pornográficas, de comercio y producción ilegal de drogas y armas, páginas web sometidas a censuras gubernamentales, que encuentran su *humus* natural en este ambiente.[27]

De acuerdo con el autor, puede señalarse además que la existencia de un vasto contenido en cuestión de bases de datos con información almacenada por gobiernos, organizaciones y entidades que no listan en los resultados de los buscadores comunes; la *Internet Profunda* refiere a un contenido que está formado por sitios donde es necesario ingresar de forma anónima y, por ende, es conveniente utilizar programas que se encarguen de ocultar la identidad evitando así posibles riesgos, los cuales se definirán más adelante.

Según la entidad *Electronic Frontier Fundation (EFF)*, el anonimato «*implica la capacidad de mantener la confidencialidad de una amplia variedad de actividades propias en línea, incluyendo la ubicación, la frecuencia de las comunicaciones, y tantos otros detalles. El anonimato en línea debe entenderse no sólo como el estado de no ser identificado por terceros, sino también como la cualidad de*

[27] Almudi. Piciarelli, Fabrizio. *El «Deep Web»: el lado oscuro de Internet. Un viaje más allá de las fronteras de la red.* España. 2017. Disponible en: https://www.almudi.org/noticias-articulos-y-opinion/11416-el-deep-web-el-lado-oscuro-de-internet-un-viaje-mas-alla-de-las-fronteras-de-la-red Fecha de consulta: 21/04/2017

ser incognoscible para terceros».[28] Es importante hacer mención de ello puesto que implica la participación libre en cualquier actividad en línea sin revelar la identidad del usuario, y además la ampliación sobre una gama de cuestiones de protección de datos, y la capacidad de controlar lo que una persona hace cuando navega en la Internet.

Además, agrega la entidad que *«la diversidad de formas en las que el anonimato en línea se protege varía desde decisiones de los individuos de no usar sus nombres legales, pasando por las políticas y prácticas de algunos intermediarios para evitar requerir el registro o uso de un nombre legal, a través de las políticas de retención de datos de los intermediarios, hasta el desarrollo y uso de herramientas de software que son diseñadas específicamente para tratar de asegurar el anonimato».*[29] Los sistemas judiciales vendrían a ser los más adecuados para equilibrar el derecho de los ciudadanos a la expresión anónima con la necesidad de proporcionar un mecanismo adecuado para regular la actividad.

1.2.2.a *TOR (The Onion Router)* o *El Enrutador Cebolla*

El navegador web *The Onion Router* o *TOR,* por sus siglas en inglés, cuya traducción al español vendría a ser «*El Enrutador Cebolla»,* según Carlos González, *«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.»*[30] Razón por la cual existe la posibilidad de eliminar el rastro de tráfico de intercambio en la navegación por Internet.

---

[28] Electronic Frontier Foundation. *Anonimato y Cifrado.* Estados Unidos. 2015. Disponible en: https://www.eff.org/files/2015/03/18/anonimatoycifrado-eff-11.pdf Página. 12. Fecha de Consulta: 21/04/2017

[29] Ibíd. Página 15

[30] ADSL ZONE. González, Carlos. *Por qué Tor funciona lento, y como se puede navegar más rápido por la Deep Web.* España. 2015. Disponible en:

Para José Pagliery, su objetivo principal radica en el desarrollo de una web de comunicaciones distribuida de baja latencia y superpuesta sobre internet en la que el encaminamiento de los mensajes intercambiados entre los usuarios no revele la identidad o dirección IP de estos, además de mantener la integridad y el secreto de la información mientras se viaja a través de ella. Además agrega que, el enrutador debutó por primera vez en el año dos mil dos como el proyecto *The Onion Routing* o *El Enrutamiento Cebolla* creado por el Laboratorio de Investigación Naval de Estados Unidos como un método para comunicarse de forma anónima en línea, lo que da la posibilidad de ocultar la dirección IP con la identidad del usuario.[31]

David Martínez, en el documento «*The Deep Web; los suburbios de Internet*» señala que los servicios que pueden encontrarse en esta plataforma son comúnmente conocido con *Hidden Services* o servicios ocultos y no van mucho más allá de los servicios que pueden encontrarse en la Internet común, pero tienen el añadido de la privacidad: foros, comercio electrónico bibliotecas de documentos en PDF o TXT, servidores de correo, etc.[32] Uno de los sitios de referencia en TOR es *«The Hidden Wiki»* o la wiki oculta, donde con mucha frecuencia los enlaces de la red cambian de TOR, buscadores internos, repositorios de documentación importante, enlaces a foros de interés, etc.[33]

1.3 Peligros y Amenazas

Como ya se ha argumentado, la Internet Profunda pese a ser desconocida por gran parte de los internautas, en realidad ha existido siempre. Sin embargo, es de hacer énfasis en la importancia que generan los riesgos que pueden existir al ingresar a un sitio el cual, por su facilidad de pasar desapercibido y libertad para generar

---

https://www.adslzone.net/2015/09/23/por-que-tor-funciona-lento-y-como-se-puede-navegar-mas-rapido-por-la-deep-web/ Fecha de Consulta: 25/02/2017

[31] Expansión. Pagliery, José. *Deep Web, el Internet que desconoces.* México. 2014. Disponible en: http://expansion.mx/tecnologia/2014/03/10/las-profundidades-del-mar-de-internet Fecha de Consulta: 23/02/2017

[32] Rebelión. Martínez, David. *The Deep Web; los suburbios de Internet*. Estados Unidos. 2013. Disponible en: http://www.rebelion.org/docs/162798.pdf Página 4. Fecha de consulta: 21/04/2017

[33] Loc. Cit.

contenido sin algún tipo de restricción, puede generar un impacto negativo en los sistemas operativos de los usuarios de Internet.

Para José Luis Espinosa, al referirse al contenido de la Internet Profunda, argumenta: «*Deep Web se sirve de toda una serie de herramientas cuya finalidad* es mantener el anonimato*, siendo las más famosa de ellas The Onion Router (TOR), una plataforma creada por el Laboratorio Naval de EE.UU., que posibilita* ocultar la dirección IP *y otros datos relacionados con la identidad del usuario, y que funciona utilizando distintos niveles -como las capas de una cebolla- de codificación.»*[34] cuyo contenido fue anteriormente desarrollado.

Esto quiere decir que este anonimato genera la posibilidad de ingresar a sitios de la Internet Profunda que, técnicamente, son inaccesibles a través de los medios tradicionales, por lo que se convierte en un lugar protegido y seguro para que cibercriminales o particulares de toda índole realicen servicios ilegales. La base es la utilización de códigos de cifrados complejos que protegen al usuario del análisis de tráfico, siendo el anonimato la principal inspiración de las mismas.

1.3.1 Actividad Ilícita en la Internet Profunda

La *Deep Web* al ser un sitio con las características que por su naturaleza permiten la realización de actividad ilícita en su mayoría, 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. Como ya se mencionó anteriormente, por David Tabóas, para describir la plataforma se utiliza la metáfora del iceberg, estimando que el setenta y cinco por ciento (75%) del contenido que transita por

[34] ABC Tecnología. Espinosa, José Luis. *Los Peligros de Deep Web, la internet profunda.* España. 2015. Disponible en: http://www.abc.es/tecnologia/redes/20150708/abci-deepweb-secretos-internet-oculta-201507072005.html Fecha de consulta: 24/02/2017

internet no se indexa en los buscadores y, por tanto, permanece oculta para el usuario común. [35]

Según el reciente informe de la entidad *Trend Micro* llamado «*Por debajo de la superficie: exploración de la Deep Web*» (*Below the Surface: Exploring the Deep Web*), más del veinticinco por ciento de vínculos entre el internet oculto y el visible tienen fines de explotación infantil y pornografía. Para obtener información de la plataforma en estudio aparentemente inexpugnable, los investigadores de esta entidad utilizaron su sistema denominado Analizador de *Deep Web,* la cual se encarga de recopilar los *URL (Uniform Resource Locator),* por sus siglas en inglés, y que en su traducción en español vendría a ser *Localizador Uniforme de Recursos* vinculadas a Deep Web, incluyendo Tor y sitios ocultos tratando de extraer información relevante vinculada a ellos. [36]

1.3.2 La *Darknet o Dark Web*

Según Juan Manuel García «l*a 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. Es un tipo de páginas de acceso muy restringido cuyo contenido está cifrado siempre, y que cambian a menudo de ubicación. Para acceder a ellas, 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.».*[37]

---

[35] Universitat Oberta de Catalunya. Tabóas, David. *¿Qué esconde la Deep Web?* España. 2016. Disponible en: https://www.uoc.edu/portal/es/uoc-news/actualitat/2016/043-deep-web.html Fecha de Consulta: 24/02/2017

[36] TrendMicro. Ciancaglini, Vincenzo y otros. *Below de Surface: Exploring the Deep Web.* Alemania. 2015. Disponible en: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf Página 8. Fecha de consulta: 03/02/2017

[37] Magazine Digital. García, Juan Manuel. *Cien horas en la Internet Profunda*. España. 2016. Disponible en: http://www.magazinedigital.net/historias/reportajes/cien-horas-en-internet-profunda Fecha de Consulta: 03/03/2017

En síntesis, según lo expone García, la *Dark Net* es invisible para el público habitual cuyo fin consiste en sentar las bases para hacer todo lo que Internet superficial no permite o no se puede hacer revelando la identidad. Esto desde el comercio de drogas que tanto preocupa a la Organización de las Naciones Unidas hasta actividades consideradas más complicadas como: venta de armas, contratación de asesinos, comercio de personas o pedofilia.

Adicionalmente, esto da a entender que no solamente conlleva tener los conocimientos necesarios para realizar la actividad ilícita puesto que se debe tener una cierta cantidad de contactos que se encarguen de abrir las puertas para desarrollar una estructura delictiva más compleja y que goce de una falta de control y regulación legal.

1.3.2.a Bitcoin

Al ser un mercado de transacciones ilegales se debe utilizar una moneda capaz de permitir el anonimato en cuanto la adquisición de la misma y desarrollo de actividades y a partir de ello nace lo que hoy en día se conoce como *Bitcoin,* cuyo término no tiene propiamente una traducción en español pero que está formado por los términos «*byte»,* anteriormente definido, y «*coin»* cuya traducción en inglés es «moneda»*.* La entidad «*Bitcoin.org»* la define como «*una red consensuada que permite un nuevo sistema de pago y una moneda completamente digital. Es la primera red entre pares de pago descentralizado impulsado por sus usuarios sin una autoridad central o intermediarios. Desde un punto de vista de usuario, Bitcoin es como dinero para Internet*.»[38]

Su origen recae, según la entidad antes citada, *«en la primera implementación de un concepto conocido como "moneda criptográfica", la cual fue descrita por primera vez en 1998 por Wei Dai donde propuso la idea de un nuevo tipo de dinero que utilizara la criptografía para controlar su creación y las transacciones, en lugar de*

[38] BITCOIN. *¿Qué es Bitcoin? Preguntas Frecuentes.* Estados Unidos. 2016. Disponible en: https://bitcoin.org/es/faq#que-es-bitcoin Fecha de Consulta: 03/03/2017

que lo hiciera una autoridad centralizada».[39] Analizando los motivos de su creación puede distinguirse claramente la necesidad que nace a partir de tener la capacidad de realizar transacciones en línea sin el control centralizado de algún Estado que regule su utilización y por lo tanto el tipo de actividades posibles en línea.

Según Juan Manuel García, si el usuario no posee un manejo prudente o los conocimientos necesarios para poder navegar en la Internet Profunda significaría perder los *bitcoins* que pueda quedar expuestos o incluso el control sobre la información personal o sobre los dispositivos. Están a la orden del día los ataques *man-in-the-middle* «*en los que un intermediario se atribuye la capacidad de interceptar las comunicaciones que se realizan desde el dispositivo de conexión a internet*» o el *ransomware* «*consistente en bloquear el acceso a partes del ordenador del usuario, como el disco duro, y pedir un rescate para liberar la información secuestrada*».[40]

Las puertas hacia la intercepción de comunicaciones y el bloqueo de acceso a los dispositivos son evidentes de las secuelas que pueden traer la navegación en la *Deep Web* sin algún tipo de conocimiento o precaución al entrar a la misma. Se encuentra expuesta la integridad de la persona y la seguridad informática del dispositivo que se utiliza para poder ingresar a ese tipo de contenido. La posibilidad de ser infectado con *virus* informáticos es mayor cuando se navega por sitios desconocidos a partir de la revelación de información personal de forma directa o indirecta, cuyo término será definido más adelante.

[39] Loc. Cit.
[40] Magazine Digital. García, Juan Manuel. *Cien horas en la Internet Profunda*. España. 2016. Disponible en: http://www.magazinedigital.net/historias/reportajes/cien-horas-en-internet-profunda Fecha de Consulta: 03/03/2017

CAPÍTULO 2

Los Delitos Informáticos

La *Deep Web,* por su naturaleza es una plataforma virtual, capaz de proporcionar las facilidades para desarrollar distintas actividades catalogadas como ilícitas, y, por consiguiente, denominadas como delitos. Para profundizar sobre el tema, a continuación, se desarrollará lo relacionado con este tipo de actos, puesto que valiéndose de la libertad de acceso y anonimato pueden ser posibles a través de ella.

2.1. Concepto de Delitos Informáticos

El delito puede ser catalogado como toda actividad punitiva del Estado y ha recibido denominaciones a través de la historia las cuales se encuentran en una constante adaptación para la sociedad actual, esto crea una abundancia de formas para definir el término "delito", que sostienen conceptos simples hasta más complejos pero que atienen a diferentes corrientes de pensamiento por la vasta información obtenida a través del tiempo por distintos autores y profesionales del derecho.

El término delito, según los autores José Francisco de Mata Vela y Héctor Aníbal De Léon Velasco citando a Luis Jiménez de Asúa, se refiere a «*un acto típicamente antijurídico, imputable al culpable, sometido a veces a condiciones objetivas de penalidad y que se haya conminado con una pena, o en ciertos casos, con determinada medida de seguridad en reemplazo de ella.»* [41] Esto obedece al principio que lo establece como una acción sancionada con una pena adecuada y suficiente.

[41] De León Velasco, Héctor Aníbal y José Francisco de Mata Vela. *Derecho Penal Guatemalteco: Parte General y Parte Especial.* Guatemala. Editorial Magna Terra. 2012. 22va. Edición. Página 132

Al tomar lo anterior en cuenta, al momento de definir el término delito informático debe relacionarse como aquellos actos delictivos que son posibles realizar a partir de la brecha que proporciona un dispositivo electrónico para poderlos desarrollar.

Para definirlo, el autor Juan Manuel García de la Cruz define el delito informático como «*toda acción culpable realizada por un ser humano que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que por el contrario produzca un beneficio ilícito a su autor, aunque no perjudique en forma directa o indirecta a la víctima. Actitudes ilícitas en que se tiene a las computadoras como instrumento o fin*»[42]. En ese orden de ideas se recalca el punto de existir una herramienta indispensable para llevar a cabo estos delitos siendo ésta un ordenador o cualquier medio electrónico que permita realizar estos actos.

Alberto Enrique Nava Garcés lo denomina como aquellas actividades criminales que, en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo o hurto, fraude, falsificaciones, perjuicios, estafa, sabotaje, etcétera.[43] Además, el autor agrega, que debe destacarse que el uso de las computadoras ha propiciado, a su vez, la necesidad de regulación por parte del derecho, para sancionar conductas que pueden ser catalogadas como ilícitas.[44]

Pablo Palazzi, citado por Nava Garcés, menciona, que *«sin establecer una regla genérica, se puede afirmar que una computadora puede constituir un medio para cometer un delito o el objeto sobre el cual recaiga el mismo».*[45] Lo cual genera la idea de expresar que el carácter antijurídico de la conducta que transmite o procesa datos de manera ilegal cuenta como uno de los elementos básicos para la comisión de este tipo de delitos.

---

[42] García de la Cruz, Juan Manuel. *Delitos Informáticos.* México. El Cid Editor. 2009. Pág. 6

[43] Nava Garcés, Alberto Enrique. *Análisis de los Delitos Informáticos*. México. Editorial Porrúa. 2005. Página 18

[44] Loc. Cit.

[45] Ibíd. Página 21

A manera más atinada, Julio Tellez Valdés lo define como «*las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin*».[46] Por otra parte, María de la Luz Lima denomina «Delitos Electrónicos» *a «cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, 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*».[47]

La relación de elementos en las definiciones anteriores ayuda a brindar una definición acerca de lo que es un delito informático, para lo cual puede mencionarse que es cualquier acción u omisión típica y antijurídica que se realiza por medio de alguna tecnología o componente de la misma que ocasione el desarrollo de actividades lesivas hacia la confidencialidad e integridad de las personas y la información.

Además, de acuerdo con De Mata Vela y De León Velasco, es importante hacer mención que existe una adecuada relación entre los juristas, sobre los elementos comunes en el delito ya que se pueden numerar como: la tipicidad, la antijuricidad y la culpabilidad. Esto obedece al tratamiento de la Teoría General del Delito que se ocupa de todos aquellos elementos comunes a todo hecho punible.[48]

Antonio Enrique Pérez Luño, citado por Nava Garcés, señala, que la difusión de la informática en todos los ámbitos de la vida social ha determinado que se le utilice como instrumento para la comisión de actividades que lesionan bienes jurídicos y entrañan un peligro social.[49] A esa cuenta Nava Garcés expresa que el problema no está en la constitución del delito, sino en la forma de probar ese delito, en la forma de establecer fehacientemente el nexo causal.[50]

---

[46] Téllez Valdes, Julio. *Derecho Informático.* Instituto de Investigaciones Jurídicas de la Universidad Nacional Autónoma de México. México. 1987. Página 105

[47] . Página 100

[48] De León Velasco, Héctor Aníbal y José Francisco de Mata Vela. *Óp. Cit.* Pág. 134

[49] Nava Garcés, Alberto Enrique. *Óp. Cit.* Página 24

[50] Ibíd. Página 25

Es por ello que se puede señalar que es común que las personas alrededor del mundo, hoy en día, se hayan convertido poco a poco en dependientes de las tecnologías como herramienta indispensable para las actividades del día a día. El avanzado crecimiento social ha logrado que una gran parte de la población mundial tenga acceso a distintos tipos de dispositivos informáticos, y por lo tanto, a la Internet. Lo que solía hacerse manualmente, ahora puede hacerse a través de medios informáticos, lo cual significa una gran ventaja; sin embargo, al mismo tiempo puede aprovecharse la tecnología para cometer actos delictivos, siendo una de las herramientas para llevar a cabo éstos, la *Deep Web.*

De acuerdo con Flores Salgado, en la mayoría de las naciones europeas existen normas similares, en relación a la sanción de delitos informáticos y estos enfoques están inspirados por la misma preocupación de contar con comunicaciones electrónicas, transacciones e intercambios tan confiables y seguros como sea posible.[51] Expresa además, que el derecho penal de los estados interesados en combatir esta a lo que se le cataloga como 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.[52]

En esta materia Nava Garcés argumenta que, «*son escasas las legislaciones locales que han incluido en sus catálogos penales los llamados delitos informáticos, menos aún que han hecho una división entre los mismos y ninguna ha considerado destacar que la computación suele ser el medio comisivo en la realización de ilícitos ya sancionados».*[53] Esto da a entender que en materia de delincuencia informática se haría una gran contribución en cuanto a la creación de legislaciones completas para que todas las formas de ataques contra los sistemas de información puedan

[51] Flores Salgado, Lucerito. *Óp. Cit.* Página 134
[52] Loc. Cit.
[53] Nava Garcés, Alberto Enrique. *Óp. Cit.* Página 75 y 76

ser objeto de investigaciones mediante técnicas y métodos disponibles en derecho penal.

En ese mismo orden de ideas Flores Salgado agrega, que referente a los autores de estos delitos, éstos deben ser identificados y llevados a juicio y los tribunales deben disponer de sanciones adecuadas y proporcionadas, ya que de esa manera se enviará así un claro mensaje disuasivo a los autores potenciales de ataques contra los sistemas de información. Además, los vacíos jurídicos y las diferencias pueden impedir una cooperación policial y judicial eficaz en caso de ataques contra sistemas de información, que por su naturaleza requieren una cooperación internacional.[54]

Por su parte, el Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos, citado por Flores Salgado, expresa que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada.[55] En síntesis, con lo anteriormente relacionado por los autores citados, debe destacarse que la delincuencia informática de un delito instrumentado por el uso de la computadora a través de la Internet.

2.2 Origen del delito informático

Cualquier acto que sea considerado delito en este campo requiere de una iniciación mediante la voluntad de uno o varios individuos cuyos fines comunes en general se logran mediante la formación de estructuras sociales conectadas mediante vínculos o relaciones de amistad, profesión o parentesco. Esto da a entender que, el delito informático surge de una secuencia lograda a partir de la ideación hasta concretar la acción que es considerada ilícita.

[54] Flores Salgado, Lucerito. *Óp. Cit.* Página 135
[55] Ibíd. Página 136

La acción juega un papel importante en la iniciación del delito informático, puesto que la conducta del ser humano dentro de una sociedad pueda causar una infracción a la norma legal vigente. Según Luis Jiménez de Asúa, puede definirse el acto como: «*Una manifestación de la voluntad que, mediante acción, produce un cambio en el mundo exterior, o que por no hacer lo que se espera deja sin mudanza ese mundo externo cuya modificación se aguarda. El acto es, pues, una conducta humana voluntaria que produce un resultado*.» [56] La acción vendría a ser la manifestación de la voluntad delictiva, o sea, que está penado por la ley.

De acuerdo a lo anterior puede señalarse que la evolución tecnológica ha logrado el surgimiento de nuevas conductas nocivas que, tomando ventaja de las facultades de las informaciones, buscan causar daño y lucros delictivos. Esta situación plantea una serie de problemáticas a la seguridad de información en distintas naciones alrededor del mundo representando una constante amenaza para el bien común y economía de algún país y para la sociedad que en su territorio se desarrolla. Tal y como fue brevemente señalado en el primer capítulo existe el riesgo de ser atacado por virus informáticos, los cuales pueden ser considerados como los pioneros a los grandes problemas que presenta la informática en su cronología.

José Luis Castillo señala en su obra *Virus Informático* que fue «*en 1949, el matemático estadounidense de origen húngaro John von Neumann, en el Instituto de Estudios Avanzados de Princeton (Nueva Jersey), (quién) planteó la posibilidad teórica de que un programa informático se reprodujera. En 1983, el ingeniero eléctrico estadounidense Fred Cohen, que entonces era estudiante universitario, acuñó el término de "virus" para describir un programa informático que se reproduce a sí mismo.*» [57]

A partir de este antecedente, se logra acuñar el concepto que hasta hoy en día se conoce como virus informático cuyo significado, según Castillo es *(…) un programa*

[56] Jiménez de Asúa, Luis. *Lecciones de Derecho Penal.* México. Editorial Mexicana. 1997. 2da. Edición. Pág. 137
[57] Castillo, José Luis. *Virus Informático.* México. El Cid Editor. 2009. Pág. 5

que tiene la capacidad de causar daño y su característica más relevante es que puede replicarse a sí mismo y propagarse a otras computadoras. Infecta cualquier archivo o sector de las unidades de almacenamiento (…)[58]*.* Esto genera las bases para las acciones nocivas informáticas para los usuarios de tecnologías, existe claramente la intención de causar daño, lo que significaría que más adelante constituirían lo que ahora se conoce como delitos informáticos en sus variaciones en distintos escenarios.

Stephanie Perrin citada por Iván Manjarrés y Farid Jiménez, menciona que el término delito informático se acuñó a finales de los años noventa, a medida que Internet se expandió por toda Norteamérica. Después de una reunión en Lyón, Francia, se fundó un subgrupo del grupo de naciones que conforman el denominado «G8» con el objetivo de estudiar los problemas emergentes de criminalidad que eran propiciados por o que migraron a Internet. El «*Grupo de Lyón»* utilizó el término para describir, de forma muy imprecisa, todos los tipos de delitos perpetrados en la red o en las nuevas redes de telecomunicaciones que tuvieran un rápido descenso en los costos.[59]

Esto marca las bases para diseñar en el año 2000 el Tratado sobre Delito Informático, el cual incorpora una nueva gama de técnicas de vigilancia que serían las consideradas para combatir el delito informático, además de las disposiciones y áreas temáticas en las que se requería legislación para regular las actividades virtuales catalogadas como delito.

2.3 Bien Jurídico Tutelado:

De Mata Vela y De León Velasco, citando al autor Jorge Palacios, expresan que «*el bien jurídico tutelado es el interés que el Estado pretende proteger a través de los*

[58] Ibíd. Pág. 8
[59] Corporación Universitaria Americana. Majarrés, Iván y Farid Jiménez. *Caracterización de los delitos informáticos en Colombia.* Colombia. 2012. Disponible en: http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/126/149 Pág. 5. Fecha de consulta: 05/03/2017

distintos tipos penales; interés que es lesionado o puesto en peligro de la acción del sujeto activo; cuando esta conducta se ajusta a la descripción legal».[60] El objeto único del delito, es el bien jurídico que el hecho punible lesiona o pone en peligro, es decir, el concreto valor elevado a interés jurídico. Esto se suma a la vital importancia que tiene esta figura para la constitución de acciones delictivas.

Este extremo deja ver que no se puede concebir un delito que no pretenda la seguridad de un bien jurídico; o sea, sirve como un elemento sobre el cual recae el interés del Estado para encuadrar cierta actividad como lesiva y de esa manera proteger los intereses dirigidos al bien común. Generalmente, de acuerdo con De Mata Vela y De León Velasco, los bienes jurídicos tutelados que pertenecen a una persona individual son: la vida, su integridad personal, su honor, su seguridad y libertad sexual, su libertad y seguridad personal, su patrimonio, su orden jurídico familiar, su estado civil, entre otros.[61]; en tanto a lo referente a personas jurídicas pueden verse amenazadas en cuanto a su patrimonio.

Francisco Muñoz Conde, citado por Nava Garcés, estipula, referente al bien jurídico, que «*la norma penal tiene una función protectora de bienes jurídicos. Para cumplir esta función protectora eleva a la categoría de delitos, por medio de su tipificación legal, aquellos comportamientos que más gravemente lesionen o ponen en peligro los bienes jurídicos protegidos.»*[62] El bien jurídico es por tanto la clave que permite darle sentido y fundamento a la naturaleza del tipo penal.

Flores Salgado señala como elemento de tipo penal el «*bien jurídico tutelado mediante la sanción de los delitos informáticos que presupone la informática y el resguardo de los medios involucrados en la computación electrónica»*[63]. Por lo tanto, se relaciona un elemento objetivo cuyo fin es dañar o causar algún perjuicio que perjudique el beneficio moral mediante del uso de los dispositivos electrónicos. En

[60] De León Velasco, Héctor Aníbal y José Francisco de Mata Vela. *Óp. Cit.* Pág. 230
[61] Ibíd. Pág. 131.
[62] Nava Garcés, Alberto Enrique. *Óp. Cit.* Página 59
[63] Flores Salgado, Lucerito. *Óp. Cit.* Pág. 132

esta materia, los autores Rolando Alvarado y Ronald Morales, clasifican por bienes jurídicos tutelados los siguientes:

1. **La Información:** Se protege la información en cuanto a sus atributos consistentes en la integridad, disponibilidad y confidencialidad.[64]
2. **El Patrimonio:** Se protege el patrimonio toda vez que se sancionan todos aquellos actos de transferencia patrimonial no consentida por el propietario, así como lo relativo al daño informático.[65]

En análisis a lo señalado por los autores anteriores, se evidencia una importancia notable en cuanto a la labor de un Estado para tratar los asuntos relacionados a seguridad informática, ya que partir de los ataques cibernéticos existe una constante amenaza hacia la estructura estratégica de los Estados relacionada con diversas áreas de interés común puesto que los delitos informáticos son capaces de trascender del mundo virtual hacia el mundo real. Como consecuencia, la creciente necesidad de regular estas actividades delictivas debe hacer que los Estados conlleven una regulación de protección de los bienes jurídicos tutelados en materia informática.

Además, en esta misma línea debe recalcarse que la Internet juega un papel como un medio anónimo que facilita el acceso e intercambio de información y datos, convirtiéndose en un instrumento de comunicación, obtención de recursos e intercambios electrónicos, lo que conlleva importantes repercusiones en los distintos sectores sociales, económicos, jurídicos y culturales, lo que lo convierte en un generador de relaciones sociales y públicas. Por lo cual, al ser un espacio que no conoce límites es propenso a ser un motor de surgimiento de irregularidades en la actividad de los usuarios de internet.

[64] Morales, Ronald y Rolando Alvarado. *Óp. Cit.* Pág. 2
[65] Loc. Cit.

2.4 Sujeto Activo

Rodríguez Devesa, citado por los autores De Mata Vela y De León Velasco, expresa que el sujeto activo es denominado como aquel que *«realiza la acción, el comportamiento en la ley. Al ser la acción un acaecimiento dependiente la voluntad, no puede ser atribuida, ni por consiguiente realizada, sino por una persona humana.»*[66].

Francisco Muñoz Conde, citado por Nava Garcés, expresa en cuanto al sujeto activo que el delito como obra humana siempre tiene un autor, aquél que precisamente realiza la acción prohibida u omite la acción esperada.[67] Agrega el citado autor, «*Normalmente en el tipo se aluda a dicho sujeto con expresiones impersonales como 'el que' o 'quien'. En estos casos, sujeto activo del delito puede ser cualquiera, al margen de que después puede ser o no ser responsable del delito en cuestión dependiendo o no las facultades psíquicas mínimas necesarias para la culpabilidad.»*[68]

Por su parte Flores Salgado, denomina al sujeto activo, en materia informática, a «*aquellas personas de un determinado nivel de inteligencia y educación, superior al común, mismos que pueden ser los programadores que violan o utilizan controles protectores del programa o sistema; los analistas en sistemas, los analistas de comunicaciones, supervisores que tiene conocimiento en operaciones de sistemas de seguridad, personal técnico y mantenimiento, etc».*[69] Dando la pauta que las posibilidades que generan las causales del delito informático son infinitas tomando en cuenta la cantidad de personas que tienen acceso a dispositivos informáticos.

En este tipo de ilícitos existe una característica infalible que corresponde a la calidad de sujeto que puede cometerlos, ya que tomando lo considerado por Flores Salgado,

---

[66] De León Velasco, Héctor Aníbal y José Francisco de Mata Vela. *Óp. Cit.* Pág. 219
[67] Nava Garcés, Alberto Enrique. *Óp. Cit.* Página 57
[68] Loc. Cit.
[69] Flores Salgado, Lucerito. *Óp. Cit.* Pág. 132

se habla de un individuo de cierto nivel intelectual y socioeconómico que ha tenido acceso al estudio del campo informático, lo cual es determinante para atribuírseles los conocimientos necesarios para realizar los actos delictivos de esta naturaleza. No podría alegarse generalmente que quienes cometen este tipo de delitos son personas que viven en una situación económica no aceptable o tengan falta de educación, ya que en la mayor parte de las veces se trata de personas que tienen habilidades y conocimientos adecuados en cuanto nivel informático.

2.5 Sujeto Pasivo

De acuerdo con De León Velasco y De Mata Vela, el sujeto pasivo del delito es una figura que corresponde al «*titular del derecho o interés que jurídicamente protege el Derecho Penal»*[70]*,* o sea, el sujeto titular del bien jurídico tutelado atacado por el delito. Esta figura significaría ser el ente sobre el cual recae la conducta de la acción u omisión que realiza el sujeto activo.

En esta materia, Flores Salgado señala que «*entre los sujetos pasivos de los delitos informáticos figuran las entidades bancarias como víctimas frecuentes por la creciente utilización de las transferencias de fondos de forma electrónica, donde se movilizan cantidades importantes de dinero mediante símbolos electrónicos como único tipo de registro.»*[71] El temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantengan al margen.

Muñoz Conde, citado por Nava Garcés, expresa, en cuanto al sujeto pasivo, *(…) esta figura es el titular del bien jurídico es el sujeto pasivo. No siempre coincide el titular del bien jurídico protegido en el tipo legal con el sujeto sobre el que recae la acción típica.(…)*[72] En el mismo sentido, se puede señalar que es mediante la

[70] De León Velasco, Héctor Aníbal y José Francisco de Mata Vela. *Óp. Cit.* Pág. 224
[71] Flores Salgado, Lucerito. *Óp. Cit.* Pág. 133
[72] Nava Garcés, Alberto Enrique. *Óp. Cit.* Página 60

divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando la sociedad virtual para tomar precauciones en cuanto la prevención de ciberdelincuencia que se lograría una efectiva protección de los derechos e intereses personales de todos los usuarios de Internet; se estaría avanzando en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

2.6 Clasificaciones del Delito Informático

Rolando Alvarado y Ronald Morales citando a Jesús Antonio Molina Salgado, refieren una clasificación de los delitos informáticos de la manera siguiente:[73]

a) **Como Instrumento o Medio:** En esta categoría se encuentran las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito.[74]
b) **Como Fin u Objetivo:** En esta categoría se encuadra a las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.[75]

Al definir el término de delitos informáticos se hacía la referencia a acciones antijurídicas que cuentan con la finalidad de causar daño a un dispositivo o sistema de programas, las cuales se sirven de éstas como medio operativo para realizar actos ilícitos. Además, de acuerdo a la real afectación al bien jurídico tutelado estos pueden ser dirigidos a vulnerar el patrimonio, propiedad intelectual o bien la privacidad o indemnidad de las personas.

[73] Ibíd. Pág. 16
[74] Loc. Cit.
[75] Loc. Cit.

Estos argumentos sirven como principios para proponer la siguiente clasificación realizada por el autor Hans Aarón Noriega Salazar[76], distinguiéndose entonces dos tipos:

1. Delitos Informáticos contra el patrimonio y la propiedad intelectual.
2. Delitos Informáticos que atentan contra la privacidad, la intimidad, la libertad o indemnidad sexual.

2.6.1 Delitos Informáticos contra el Patrimonio y la Propiedad Intelectual:

Para Noriega Salazar, los avances tecnológicos han permitido que las computadoras constituyan un medio de trabajo, comunicación y entretenimiento cada vez más usado. Es comprensible que el uso de la Internet en todos los ámbitos esté amenazado entonces por la posibilidad de comisión de hechos delictivos por esa vía, o bien a través del aprovechamiento de las facilidades que brinda.[77] El autor los denomina de la siguiente forma:

a) La copia ilegal de software, películas y música
b) Defraudaciones a través de publicidad engañosa.
c) Fraudes cometidos por medio del acceso y manipulación a sistemas informáticos bancarios o financieros.
d) Sabotaje a sistemas informáticos,
e) Uso no autorizado de sistemas informáticos ajenos.
f) Espionaje informático.
g) Falsificación de documentos por medio de la computadora.

[76] Noriega Salazar, Hans Aarón. *Delitos Informáticos.* Instituto de la Defensa Pública Penal. Guatemala 2011. Página 24. Disponibilidad y acceso en: http://descargas.idpp.gob.gt/Data_descargas/Modulos/delitosinformaticos.pdf Consultado el 05/03/2017

[77] Ibíd. 24 y 25

2.6.2 Delitos Informáticos que atentan contra la Privacidad, la Intimidad, la Libertad o Indemnidad sexual: Noriega Salazar clasifica las acciones u omisiones en que incurre el sujeto activo y que lesionan o ponen el bien jurídico tutelado privacidad, entendida ésta, como el ámbito de la vida privada y del cual se tiene derecho a proteger de cualquier intromisión.[78] En esta clasificación se aprecian las siguientes conductas:

a) Violación a la privacidad de la información personal o a las comunicaciones; que se refiere a las conductas tendientes a la captura o interceptación de información o mensajes ajenos.[79]

b) La Revelación indebida de información personal; delito en el que se incurre por la revelación o publicación de la información ajena obtenida con o sin ánimo de lucro.[80]

c) Pornografía infantil a través de Internet; que implica la grabación y distribución por medio de la red de imágenes de contenido sexual de niños, niñas o adolescentes.[81]

[78] Ibíd. Pág. 27
[79] Loc. Cit.
[80] Loc. Cit.
[81] Loc. Cit.

CAPÍTULO 3

Legislación

En términos generales, la Deep Web ha sido considerada como un lugar inseguro, que no ofrece seguridad o protección directa hacia los usuarios. Lo cual viene a ser 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 Salgado 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.*»[82] Esto a su vez obedece a la necesidad de entender la disposición de los autores de la actividad ilícita para adecuar y proporcionar sanciones concretas.

Al respecto la Organización de las Naciones Unidas –ONU- señaló[83]: «*La creciente densidad de tecnologías de la información y las comunicaciones también aumenta la frecuencia de la delincuencia informática nacional, obligando a las naciones a establecer legislación nacional. Puede que se requieran leyes nacionales adaptadas a la delincuencia cibernética para responder eficazmente a las peticiones externas de asistencia o para obtener asistencia de otros países. Cuando se elabora legislación, la compatibilidad con las leyes de otras naciones es una meta esencial;*

[82] Flores Salgado, Lucerito. *Óp. Cit.* Pág. 134

[83] Organización de las Naciones Unidas, Oficina Contra la Droga y el Delito. Boletín Informativo Undécimo Congreso Sobre la Prevención del Delito y la Justicia Penal 18 al 25 de Abril 2005 Bangkok Tailandia. Austria. 2005. Disponibilidad y acceso en: http://www.unis.unvienna.org/pdf/05-82113_S_6_pr_SFS.pdf Fecha de Consulta: 13/02/2017

la cooperación internacional es necesaria debido a la naturaleza internacional y transfronteriza de la delincuencia informática.»

La ONU expresa que, los ataques son transnacionales por su propia naturaleza y requieren una cooperación internacional. La uniformidad de las legislaciones debe mejorar la incursión del Estado para controlar la actividad delictiva mediante una investigación penal eficaz.[84] Debido a lo anterior, ha surgido la necesidad de aplicar la materia penal común de ámbito internacional para brindar protección a la comunidad frente a la delincuencia informática, lo cual a su vez debe crear un marco regulatorio efectivo en su aplicación para mejorar la cooperación internacional ya que en muchos países no se cuenta aún con una regulación legal que vele por los derechos de los usuarios informáticos en la red.

3.1 La Cooperación Penal Internacional

La Cooperación Penal Internacional está involucrada en la persecución penal a nivel global para la regulación y sanción de las actividades ilícitas que puedan ser realizadas en Internet. Los cuerpos normativos emitidos por distintas organizaciones y Estados son necesarios para combatir los ataques cibernéticos hacia los sistemas de información que forman parte de las comunidades virtuales. Para Noriega Salazar, esta necesidad logra en sí crear una cooperación internacional encargada de establecer mecanismos efectivos para prevención y erradicación de cualquier actividad a la que se le puede atribuir características que las vuelvan ilícitas.[85]

De acuerdo con Arroyo Zapatero y Nieto Martín «L*a cooperación judicial es la parte del Derecho Internacional Penal que se ocupa de establecer y regular los mecanismos a través de los cuales los Estados se prestan asistencia con el fin de*

[84] Ibíd. Pág. 135
[85] Noriega Salazar, Hans Aarón. *Delitos Informáticos.* Instituto de la Defensa Pública Penal. Guatemala 2011. Página 55. Disponibilidad y acceso en: http://descargas.idpp.gob.gt/Data_descargas/Modulos/delitosinformaticos.pdf Consultado el 14/02/2017

favorecer el desarrollo de un proceso penal o la ejecución de una sanción.»[86] En resumen, el término comprende la colaboración en tres áreas distintas: a) con el procedimiento penal que se desarrolla en otro Estado; b) con el fin de ejecutar una sanción impuesta por otro Estado y c) con el fin de establecer qué ordenamiento resulta mejor situado para llevar a cabo un determinado proceso.[87]

En relación a lo señalado con Arroyo y Nieto, se puede recabar que la determinación del poder penal en un Estado debe realizarse mediante el uso en conjunto de sistemas que atañen el estudio de la comisión de delitos, características del delincuente y del lugar de los hechos según su naturaleza. Analizando esto, debe expresarse que la Deep Web en términos generales, por su susceptibilidad a la comisión de ilícitos por sus características definidas en el primer capítulo, entra en un área de estudio penal internacional fuera de lo común debido a inclusión de factores que hacen difícil realizar una efectiva persecución penal en esta plataforma a diferencia de lo que se puede hacer en la red superficial.

Esto comprueba que la cooperación internacional es clave para brindarle una solución a la problemática de la criminalidad moderna transnacional, eso da la pauta a concluir que este sistema se encuentra en constante evolución y la colaboración entre Estados se hace cada vez más necesaria para combatir las amenazas informáticas. Arroyo y Nieto señalan que «*la complejidad de este tipo de colaboración depende fundamentalmente del grado de restricción de derechos que implique para un ciudadano el acto de colaboración solicitado».*[88] Por lo que existen riesgos para el derecho fundamental a la protección de datos inherentes en la red abierta en cuanto al intercambio de información lo que causa dificultad en la eficacia de los controles normativos.

[86] Arroyo Zapatero, Luis y Adán Nieto Martín. *Código de Derecho Penal europeo e internacional*. España. Ministerio de Justicia de España. 2008. Pág. 25
[87] Loc. Cit.
[88] Pág. 26

En la misma línea del análisis anterior, también cabe mencionar que la ineficacia de los controles normativos viene a significar el incremento de la importancia sobre la creación de medidas para la protección de los usuarios y sistemas informáticos, sobre todo por la facilidad con que las consecuencias de estos repercuten en la vida real, siendo la Internet una de las herramientas que proporciona libertades que en ocasiones salen de una esfera legal para entrar en la ilegal.

3.2 Convenios Internacionales

Con el fin de apoyar la cooperación internacional se han creado normativas jurídicas que permitan la regulación de la plataforma informática para evitar la realización de ilícitos.

3.2.1 Convenio de Budapest

De acuerdo con Alvarado y Morales, el Consejo de Europa, en vista a la necesidad de emitir un cuerpo normativo acertado, promulga el denominado el Convenio de Ciberdelincuencia el 23 de noviembre de 2001 al cual también se le llama como Convenio de Budapest.[89] El Consejo de Europa, el cual nace tras la Segunda Guerra Mundial con el objetivo de erigirse como guardián de los valores democráticos en el continente europeo. Esto significa el favorecimiento en Europa para abrir un espacio democrático y jurídico común, organizado alrededor del Convenio Europeo de los Derechos Humanos y de otras fuentes sobre la protección del individuo. [90]

Concorde con Alvarado y Morales, las conductas ilícitas, reguladas en el Convenio de Budapest, son: el acceso ilegal, interceptación ilegal, interferencia de los datos, interferencia del sistema uso erróneo de dispositivos, falsificación del ordenador,

[89] Alvarado, Rolando y Ronald Morales. *Óp. Cit.* Página 11.
[90] Gobierno de España. Ministerio de Asuntos Exteriores y Cooperación. *Historia y Actividad del Consejo de Europa.* España. 2016. Disponibilidad y acceso en: http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/ConsejoDeEuropa/Paginas/HistoriaActividadConsejoEuropa.aspx Fecha de Consulta: 11/03/2017

fraude del ordenador y pornografía infantil.[91] En su texto regula disposiciones sobre uniformidad de la terminología relacionada al ámbito de la informática. Además, describe las disposiciones referentes a los delitos informáticos en cuanto a los elementos que deben ser tomados a las legislaciones propias de los países que están suscritos al Convenio y sobre procesos y competencias para la persecución penal relacionados con la asistencia jurídica internacional.

Por lo citado anteriormente, debe decirse que este instrumento materializa un marco de cooperación internacional enfocado en la creación de mecanismos para prevenir y sancionar la comisión de la actividad ilícita en la red, lo cual está apegado a el tipo de contenido permitido en la Internet Profunda, ya que, según lo expuesto en los capítulos anteriores, abre una ventana de posibilidades para establecer situaciones caracterizadas por la falta de control normativo estatal creando el surgimiento de la exclusividad virtual que poseen los usuarios que manejan conocimientos informáticos.

Alvarado y Morales 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. Alvarado y Morales afirman que lo anterior, al contrario, permite tanto a Europa como para los países de América Latina y todos los países del mundo, debido a la naturaleza transfronteriza de los delitos informáticos, la normativa se convierte en un derecho positivo cuanto mayor sea el número de países se adhieran a la Convención.[92]

Guatemala, actualmente, no es parte de la Convención de la Ciberdelincuencia, sin embargo, si llegase a ser parte este cuerpo normativo vendría a significar el inicio de una nueva etapa de regulación hacia la ciberdelincuencia puesto que el estado guatemalteco no ha llegado a tener normativa concreta sobre la temática informática, la cual se encuentra en constante evolución conforme el paso del tiempo.

[91] Alvarado Rolando y Ronald Morales. *Óp. Cit.* Pág. 11
[92] Ibíd. Pág. 12

3.2.2 Convenio No. 108 del Consejo de Europa de 28 de enero de 1981, para la protección de las Personas con respecto tratamiento automatizado de datos de carácter personal.

Noriega Salazar indica que «*muchos de los delitos informáticos van dirigidos a vulnerar el bien jurídico tutelado intimidad de la persona, es decir su derecho a la vida privada. «De esa cuenta dada la preocupación existente de esta nueva forma de delinquir algunos países europeos dispusieron unificar esfuerzos, conductas y estrategias para proteger a las personas en el ámbito del tratamiento automatizado de datos de carácter persona».* [93] Esto quiere decir que, debe existir una preeminencia del derecho hacia las libertades fundamentales de los seres humanos teniendo en cuenta la facilidad de traspasar fronteras para los datos personales que son susceptibles a la perpetración de actividad ilícita.

Según el artículo 1 de este cuerpo normativo su objetivo y fin es: "*Garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona (protección de datos).*"[94]

De acuerdo con el citado artículo, debe hacerse mención acerca de la época en la cual se elaboró dicho cuerpo normativo ya que la actividad informática en la década de los ochenta no era común. Analizando su objetivo y fin puede determinarse el carácter de prevención y sanción que se le brinda a las conductas delictivas de la comunidad virtual que en la actualidad ha sido un tema de suma importancia. La normativa de esta manera logró sentar las las bases para establecer el compromiso que deben adquirir los estados para fijar las medidas y sanciones hacia las

[93] Noriega Salazar, Hans Aarón. *Óp. Cit.* Página 56.
[94] Estados Miembros del Consejo de Europa. *Convenio No. 108 del Consejo de Europa, de 28 de Enero de 1981, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal.* 1981. Artículo 1

infracciones de ley y la regulación de parámetros de protección, así como la obligación de los Estados para constituir un punto de partida sobre la prevención de ilícitos informáticos a través de la emisión de normas efectivas.

3.2.3 Decisión Marco 2005/222/JAI

Noriega Salazar señala que en fecha 24 de febrero de 2005, la Unión Europea suscribió en Bruselas, Bélgica este cuerpo normativo teniendo como objeto el reforzamiento en la cooperación internacional entre las autoridades judiciales en los ámbitos de ejecución penal a los ilícitos informáticos. Los Estados miembros en armonía hacia la búsqueda del bien común en la red involucran una aproximación de sus normas penales para la regulación de la materia.[95]

De acuerdo con el Considerando II del cuerpo normativo en cuestión, su promulgación genera una vinculación de los sistemas de persecución penal hacia los ataques de los sistemas de información como consecuencia de la amenaza de la delincuencia organizada frente a las probabilidades de existir ataques terroristas hacia los Estados miembros poniendo en peligro la realización de una sociedad de la información segura.[96] Asimismo, unifica criterios para definir delitos informáticos, entre ellos, el acceso ilegal, intromisión ilegal de datos e información. Cabe señalar que los Estados que suscriben la decisión de señalar penas efectivas distinguiendo la gravedad de los ilícitos cometidos.

3.3 La Organización de las Naciones Unidas y la Prevención del Delito Informático.

La ONU ha desarrollado estrategias y normativa para la regulación de actividades informáticas y entre ellos se encuentran:

---

[95] Noriega Salazar, Hans Aarón. *Óp. Cit.* Pág. 57

[96] Estados Miembros de la Unión Europea. *Decisión Marco 2005/222/JAI.* Bélgica. 2005. Considerando II. Disponibilidad y acceso en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:ES:PDF Fecha de Consulta: 12/03/2017

3.3.1 Declaración de Viena sobre la Delincuencia y la Justicia frente a los retos del siglo XXI

Noriega Salazar comenta sobre esta Declaración que, en la sesión plenaria 81ª de fecha 4 de diciembre de 2000 la Asamblea General de las Naciones Unidas aprobó la resolución número 55/59 sobre delincuencia y justicia frente a los retos del siglo veintiuno. Además agrega, que este instrumento tiene como punto de reflexión o de partida la preocupación de los Estados miembros con respecto al impacto, gravedad y cantidad de delitos de trascendencia internacional, la delincuencia organizada, la necesidad de generar políticas comunes de prevención y sanción de este tipo de ilícitos.[97]

La Asamblea General de las Naciones Unidas, en el cuerpo normativo, sobre lo referente a los delitos informáticos expresa: «*Decidimos formular recomendaciones de política orientadas a la acción para la prevención y el control de los delitos relacionados con la informática e invitamos a la Comisión de Prevención del Delito y Justicia Penal a que emprenda trabajos a este respecto, teniendo en cuenta la labor en curso en otros foros. Nos comprometemos también a esforzarnos por aumentar nuestra capacidad de prevenir, investigar y enjuiciar los delitos de alta tecnología y relacionados con la informática.*»[98]

En análisis a lo argumentado por la Asamblea se puede relacionar que la creación de esta norma parte de la necesidad a nivel mundial con lo relacionado a los delitos informáticos que se reflejan hoy en día de manera exponencial en cuanto a las facilidades que la red brinda ahora para desarrollar ilícitos. Por otro lado, existe una puntualización en darle uniformidad a los criterios de persecución penal y la regulación de conductas de carácter criminal, así como su prevención y sanción de éstos.

---

[97] Noriega Salazar, Hans Aarón. *Óp. Cit.* Pág. 59

[98] Asamblea General de las Naciones Unidas. *Declaración de Viena sobre la delincuencia y la justicia: frente a los retos del siglo XXI.* Resolución 55/59. 17 de enero de 2001.

3.3.2 Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos

Al respecto, Noriega Salazar señala, que el presente cuerpo normativo expresa acerca de los delitos informáticos como aquella forma moderna en que se constituyen las formas de criminalidad internacional. Señala como causales de estas necesidades una realidad caracterizada por la falta de acuerdos globales acerca de qué conductas tipo deben constituir delitos informáticos, falta de leyes especializadas en materia procesal, sustantiva, así como de investigación. el carácter transnacional de delitos cometidos mediante el uso de computadoras, ausencia de tratados de extradición, de acuerdos y de mecanismos sincronizados que permitan la plena eficacia de la cooperación internacional. [99]

3.3.3 Tratado de la Organización Mundial de la Propiedad Intelectual Sobre el Derecho de Autor

Al tomar en consideración lo detallado por Noriega, la Organización Mundial de la Propiedad Intelectual (OMPI) es un organismo especializado de la Organización de las Naciones Unidas su objetivo es “desarrollar un sistema de propiedad intelectual, que sea equilibrado y accesible y recompense la creatividad, estimule la innovación y contribuya al desarrollo económico, salvaguardando a la vez el interés público.” Los países que le conforman suscribieron el 20 de diciembre de 1996 en Ginebra el Tratado sobre derechos de autor.[100]

El Tratado de la OMPI sobre Derecho de Autor (WTC), según la entidad antes señalada, es un arreglo particular adoptado en virtud del Convenio de Berna que trata de la protección de las obras y los derechos de sus autores en el entorno digital. Además, el Tratado también se ocupa de dos objetos de protección por derechos de autor, siendo éstos: los programas de computadora y las compilaciones de datos

[99] Noriega Salazar, Hans Aarón. *Óp. Cit.* Pág. 60
[100] Loc. Cit.

u otros materiales.[101] Su artículo 14 establece: «*que los Estados regularán en sus respectivas legislaciones normativa que tienda a proteger los derechos de autor así como incluir recursos ágiles que prevengan las infracciones al derecho de autor y recursos que constituyan un medio eficaz de disuasión de nuevas infracciones*».[102]

Por tanto, debe dársele la importancia pertinente a los Estados miembros para que se encarguen de la regulación y tipificación de delitos que afecten principalmente, según el citado cuerpo legal, a la propiedad intelectual. Guatemala se encuentra entre los Estados miembros que han suscrito este tratado.

3.4 Territorialidad y Alcance de la Ley Penal

Al referirse a la ley penal en el espacio, se hace con el fin de darle una explicación al área de aplicación que puede tener la normativa penal en determinado territorio. Para Mata Vela y De León Velasco, la determinación espacial de validez de la Ley Penal es el resultado de un conjunto de principios jurídicos que fijan el alcance de la validez de la ley penal del Estado con relación al espacio, siendo más amplio que el territorio como como concepto jurídico, ya que está limitado por fronteras.[103] La ley Penal de un Estado busca en términos generales regular hechos que pueden llegar a ser cometidos fuera del área de su jurisdicción y esto ocurre de manera puntual con la actividad en la Internet ya que como se refirió en el primer capítulo es un lugar que no consiste en espacio territorial, no geográfico atado por la cuerda de las soberanías.

La territorialidad entra como principio determinante para explicar qué alcance merece la ley penal en cierto territorio y es que esta se atribuye a los límites del

---

[101] Organización Mundial de la Propiedad Intelectual (OMPI). *Tratado de la OMPI sobre el derecho de autor*. Suiza. 2016. Disponibilidad y acceso en: http://www.wipo.int/treaties/es/ip/wct/ Fecha de consulta: 12/03/2017

[102] Organización Mundial de la Propiedad Intelectual (OMPI). *Tratado de la Organización Mundial de la Propiedad Intelectual sobre Derechos de Autor.* 20 de Diciembre de 1996. Artículo 14.

[103] Mata Vela, José Francisco y Héctor Aníbal de León Velasco. *Óp. Cit.* Pág. 107

territorio del Estado que la emite. El artículo 4º del Código Penal guatemalteco, al respecto, establece que, en cuanto la Territorialidad de la Ley Penal, «*Salvo lo establecido en tratados internacionales, este Código se aplicará a toda persona que cometa delito o falta en el territorio de la República o en lugares o vehículos sometidos a su jurisdicción*».[104] Debe entenderse por ello que debe aplicarse la ley penal a individuos que cometan delitos sin importar su condición nacional o extranjera o el sistema de punibilidad de otro Estado.

En particular excepción al principio de territorialidad, existe una corriente que avala que la ley penal de un país, si puede aplicarse, a delitos cometidos fuera de su territorio, y según Mata Vela y De León Velasco esto obedece al Principio Universal o de la Comunidad de Intereses, ya que «*sostiene que la Ley Penal de cada Estado tiene validez universal, por lo que todas las naciones tienen derecho a sancionar a los autores de determinados delitos, no importando su nacionalidad, el lugar de comisión del delito ni el interés jurídico vulnerado; la única condición es que el delincuente se encuentre en territorio de su Estado y que no haya sigo castigado por este delito.»*[105]

En análisis de lo anterior, debe tomarse en cuenta la existencia de los intereses universales en cuanto la regulación y prevención de las actividades realizadas en la Internet puesto que, jurídicamente, es una temática que no es restringida en su totalidad para promover la globalización mediante esta herramienta.

3.5 Legislación Guatemalteca

Noriega Salazar señala que en la década de los años ochenta en Guatemala se comienza a acentuar la utilización de las computadoras tanto en el ámbito comercial como gubernamental, aparecen las primeras computadoras personales, así como carreras específicas en la materia tanto a nivel vocacional como universitario. Al inicio de la década siguiente se dieron los primeros pasos en investigación para la

[104] Congreso de la República de Guatemala. Código Penal. Decreto 17-73. Artículo 4.
[105] Mata Vela, José Francisco y Héctor Aníbal de León Velasco. *Óp. Cit.* Pág. 109

comunicación global a través del correo electrónico e Internet, lo cual implicaría a partir de estos acontecimientos de avance tecnológicos la vulneración de nuevos bienes jurídicos tutelados, así como innovadoras modalidades de comisión de hechos delictivos.[106]

Como consecuencia se consideró necesario realizar reformas al Código Penal a efecto de prohibir y sancionar las conductas relacionadas. De esa forma el Congreso de la República introduce modificaciones a la ley sustantiva penal a través del Decreto 33- 96 publicado en fecha 21 de junio de 1996.

En la normativa referida como motivación de la misma se expone: «Que los avances de la tecnología obligan al Estado a legislar en bien de la población de derechos de autor en materia informática tipos delictivos que nuestra legislación no ha desarrollado»[107]. En ese sentido en materia de delitos informáticos se regulan los tipos siguientes:

a) Artículo 274 “A” Destrucción de Registro Informáticos
b) Artículo 274 “B” Alteración de programas
c) Artículo 274 “C” Reproducción de Instrucciones o programas de Computación
d) Artículo 274 “D” Registros Prohibidos.
e) Artículo 274 “E” Manipulación de Información
f) Artículo 274 “F” Uso de Información
g) Artículo 274 “G” Programas Destructivos

Noriega Salazar recalca además que el Código Penal guatemalteco tipifica como ilícitas otras conductas en las que podrían subsumirse actos catalogados como delitos informáticos que consistirían en los siguientes:[108]

[106] Noriega Salazar, Hans Aarón. *Óp. Cit.* Página 35.
[107] Congreso de la República de Guatemala. Decreto 33-96. Reformas al Decreto 17-73, Código Penal. Considerando IV
[108] Noriega Salazar, Hans Aarón. *Óp. Cit.* Página 35.

a) «*Violación a Derechos de Autor contenida en el artículo 274 del Código Penal.*
b) *Violación a los Derechos de Propiedad Industrial contenida en el artículo 275 del Código Penal.*
c) *Violación a la intimidad sexual contenida en el artículo 190 del Código Penal.*
d) *Producción de pornografía de personas menores de edad contenida en el artículo 194 del Código Penal.*
e) *Comercialización o difusión de pornografía de personas menores de edad contenida en el artículo 195 Bis*
f) *Comercialización de Datos Personales ilícito penal contenido en la Ley de Acceso a la Información Pública, artículo 64.*»[109]

3.5.1 Iniciativa de Ley No. 4055: *Ley de Delitos Informáticos*

Actualmente Guatemala no cuenta con legislación especial que regule normas relativas a los delitos informáticos cometidos a través de sistemas que utilicen tecnologías de la información. Concretamente sólo lo establecido en el Código Penal es la ley vigente ante esta materia.

Sin embargo, en fecha 18 de agosto del año 2009, el Honorable Pleno del Congreso de la República conoció la iniciativa número 4055, denominada "Ley de Delitos Informáticos", misma que fue remitida para su estudio y dictamen a la Comisión de Legislación y Puntos constitucionales.[110] Dicha iniciativa busca crear una normativa de prevención y sanción de los delitos informáticos para brindar protección e inviolabilidad a los derechos de toda persona en cuanto a la confidencialidad, integridad y disponibilidad de datos y tecnologías de la información.

[109] Loc. Cit.
[110] Congreso de la República de Guatemala. *Proyecto de Ley No. 4055. Ley de Delitos Informáticos.* Disponibilidad y acceso en:http://old.congreso.gob.gt/archivos/iniciativas/registro4055.pdf Fecha de Consulta: 12/03/2017

Esto constituye, además, la finalidad de crear un marco jurídico que esté concorde a los convenios internacionales sobre ciberdelincuencia que son de naturaleza transnacional. En su parte considerativa la iniciativa pretende crear normas especiales que sean suficientes para prevenir y sancionar las conductas de cibercrimen que no tienen fronteras, ni poseen lenguaje específico, y que se realizan en un espacio virtual o ciberespacio.

La iniciativa señala que es indispensable la aprobación de una ley especial que contenga disposiciones que tiendan a proteger los derechos de toda persona en cuanto a su integridad, disponibilidad y confidencialidad de los sistemas que utilicen tecnologías de la información y sus componentes.[111] Además, señala que el Estado de Guatemala para poder contrarrestar los ataques cibernéticos debe crear normas para prevenir y sancionar esas acciones, las cuales deben ser congruentes con la normativa internacional.[112]

En análisis de lo anterior, cabe mencionar que es importante sobre todo que ante la creciente comunidad virtual y adaptación de la sociedad hacia nuevas tecnologías que cada día se actualizan según las necesidades modernas, no debe pasarse por alto, para cualquier Estado, la regulación de la actividad informática en cualquiera de sus plataformas. Esto también va relacionado con el aporte que da la Internet en beneficio de incrementar el alcance de los intereses de un individuo quien tendrá a su disposición cualquier información y contenido que desee, sin embargo, por el margen de libertad que la red maneja este contenido puede ser perjudicial para la integridad personal y de los Estados.

Según señala Alvarado y Morales, a esta iniciativa se le otorgó dictamen favorable por parte de Comisión de Legislación y Puntos Constitucionales al considerarla viable, oportuna, conveniente y constitucional, concluyendo que cubre en buena medida las necesidades legales existentes con respecto a la tipificación de los delitos relacionados con el cibercrimen y tomando en cuenta que Guatemala

[111] Ibid. Considerando I.
[112] Ibíd. Considerando III.

requiere una normativa de índole procesal en la coordinación internacional e inter-constitucional sobre la temática de delitos informáticos.[113] De momento, este ha sido el último punto que se ha trabajado en cuanto a la presente iniciativa.

3.5.2. Iniciativa de Ley 5254: *Ley contra la ciberdelincuencia*

El 9 de marzo de 2017 el pleno del Congreso de la República de Guatemala conoce la iniciativa de ley 5254, la cual se le denomina *Ley Contra la Ciberdelincuencia,* la cual en su parte de Exposición de Motivos expresa:

"*La sociedad guatemalteca no es ajena a los avances cotidianos, los negocios y las actividades financieras, utilizando para ello sistemas o redes informáticas para transmitir e intercambiar datos por internet dentro de una comunidad global… sin embargo han surgido actividades que deberían considerarse ilícitas, como lo hace otros países, por el abuso en el uso de tecnologías… estas nuevas formas de criminalidad surgen y evolucionan por la complejidad de aspectos que requieren atención por parte de los legisladores para desarrollar un cuerpo normativo adecuado que evite la impunidad de los ilícitos en cualquiera de sus formas".*[114]

En concordancia con lo expuesto en el párrafo anterior, se evidencia la necesidad innegable de la creación de un cuerpo normativo aplicable para la regulación de la actividad ilícita informática. Si bien es cierto, debe existir una ley que permita que impulse la protección de las víctimas de ataques informáticos, además, limitar y reducir la comisión de aquellas figuras delictivas de alcance global cuyo medio principal para su propicio es el internet. Por otra parte, es muy importante valerse de los medios adecuados para identificar a las personas y organizaciones que transgreden la integridad de los usuarios de internet bajo la figura de delitos

[113] Alvarado, Rolando y Ronald Morales. *Óp. Cit.* Página XII.
[114] Congreso de la República de Guatemala. *Iniciativa de Ley Número 5254* "*Ley contra la Ciberdelincuencia" Exposición de Motivos.* Disponibilidad y acceso en: http://old.congreso.gob.gt/archivos/iniciativas/registro5254.pdf Consultado el 04/11/2017

cibernéticos, para lo cual la normativa en cuestión debe velar por una estructura de protección regulada para garantizar la seguridad de los ciudadanos en la red.

3.6 Derecho Comparado

Para el estudio en materia sobre el derecho comparado se hace relación a las siguientes normativas, de acuerdo con el país de su origen:

3.6.1 España

En el Derecho Español, cabe destacar el Código Penal que fue aprobado por la ley orgánica del 23 de noviembre de 1995. (Ley Orgánica 10/1995), al ser la norma en la que tipifican y desarrollan las actividades ilícitas posibles en la Deep Web. Pueden dividirse, en 5 grandes categorías de la siguiente forma:[115]

1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos – Artículos 197 a 201.
2. Delitos informáticos: falsedad documental (Artículos 386 a 400 bis), sabotaje informático(Artículo 264 a 264 quater) y estafa o fraude informático (Artículos 248 a 251 bis).
3. Delitos relacionados con el contenido: de índole sexual, en gran medida pornografía infantil – Artículos 183 a 183 quater, artículos 187 a 190 .
4. Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines – Artículos 270 y siguientes del Código Penal.
5. Delitos por actos de índole racista y xenófoba cometidos por medios de sistemas informáticos – Artículo 510 y siguientes del Código penal.

Otros delitos que pueden desarrollarse en el ámbito digital: amenazas y coacciones (Artículos 169 a 172) y calumnias e injurias – (Artículos 205 a 216).

[115] Jefatura de Estado de España. Ley orgánica 10/1995, de 23 de noviembre. Código Penal de España.

3.6.2 Estados Unidos

De acuerdo con el Departamento de Informática de la Universidad Técnica Federico Santa María, ante la situación de amenaza constante a los medios informáticos los Estados Unidos de América han emitido leyes y reglamentos que permiten regular el uso de Internet a nivel federal y de cada estado de la unión. Cabe mencionar con que, con los hechos del 11 de septiembre del 2001, las medidas de seguridad se incrementaron y ahora las sanciones son más enérgicas. A continuación, se mencionan algunas leyes relacionadas a temas como: privacidad, seguridad, protección de datos, nombres de dominio, spam, comercio electrónico, entre otros. [116]

1. **Electronic Communications Privacy Act (ECPA). · "Ley de privacidad en las comunicaciones electrónicas, vigente desde 1986":** El código de E.E.U.U. define a las comunicaciones electrónicas como cualquier transferencia de muestras, de señales, de la escritura, de imágenes, de sonidos, de datos, o de la inteligencia de cualquier naturaleza transmitida en entero o en parte por un alambre, una radio, foto electrónica o el sistema óptico de la foto que afecta comercio de un estado a otro o extranjero. La ECPA prohíbe el acceso ilegal y ciertos accesos del contenido de la comunicación, además evita que las entidades del gobierno requieran el acceso de comunicaciones electrónicas sin procedimiento apropiado.[117]

2. **Acta Federal de Abuso Computacional.** "**Ley Federal de Abuso Computacional de 1994, modificó a la ley vigente de 1986":** De acuerdo con lo detallado por el citado Departamento de Informática, esta normativa tiene la finalidad de eliminar los argumentos hiper-técnicos acerca de qué es y que no es un virus, un gusano, un caballo de Troya y en que difieren de los

[116] Universidad Técnica Federico Santa María. Departamento de Informática. *Legislación acerca del uso de Internet.* Chile. 2014. Página 1. Disponibilidad y acceso en: www.inf.utfsm.cl/~lhevia/asignaturas/infoysoc/topicos/Etica/8_legislacion_acerca_uso_internet.pdf Fecha de Consulta 07/02/2017

[117] Loc. Cit.

virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, a los sistemas informáticos, a las redes, información, datos o programas. · Especifica la diferencia del contagio de virus realizado con intención y sin intención.[118]

3.6.3 Argentina

Según Marcelo Gabriel Ignacio Temperini, a partir de junio de 2008, la Ley 26.388 conocida como la “ley de delitos informáticos” ha incorporado y realizado una serie de modificaciones al Código Penal argentino. Es decir, la misma no regula este tipo de delitos en un cuerpo normativo separado del Código Penal con figuras propias o independientes, sino que dicha ley modifica, sustituye e incorpora figuras típicas a diversos artículos del CP actualmente en vigencia. Se modificó el Epígrafe del Capítulo III cuyo nuevo título es "Violación de Secretos y de la Privacidad", Los artículos que modifica o agrega son: 128, 153, 153 bis, 155, 157, 157 bis, 173, 183, 184, 197, 255. El art. 157 bis ya había sido incorporado por la Ley 25.326 de Protección de Datos Personales (2000) pero fue modificado por la Ley 26.388.[119]

3.6.4 Colombia

Temperini señala que, la ley 1.273, de reciente sanción legislativa (año 2009), modifica el Código Penal, creando un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos”. Se afirma que dicha normativa busca preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones. A través de esta incorporación, suma el CAPITULO I, titulado "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", a partir del cual regula una serie de artículos penales que van desde el artículo 269A hasta el artículo 269J.[120]

---

[118] Loc. Cit.
[119] Temperini, Marcelo Gabriel Ignacio. *Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1era. Parte.* Argentina. 2013. Página 5 Disponibilidad y acceso: http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf Fecha de Consulta: 16/02/2017
[120] Ibíd. Página 6

3.6.5 México

De acuerdo con Temperini, mediante reformas se crearon en el Código Penal Federal, los artículos 211 bis 1 al 211 bis 7, que buscaron tipificar los delitos informáticos clásicos teniendo en consideración la fecha de su incorporación. Se destaca la diferente que atentan contra los sistemas de cómputo que pueden o no, ser parte del sector financiero mexicano. Es importante destacar, que algunos Estados Mexicanos tienen además sus propias normas penales, incorporando otros delitos informáticos no analizados en este trabajo.[121]

[121] Loc. Cit.

CAPÍTULO 4

Análisis de Normatividad Guatemalteca Específica hacia el Derecho Convencional

En relación a lo descrito en el capítulo anterior, es menester verificar el encuadre que tiene la normativa en la materia de estudio en el ámbito interno.

4.1 Normativa Nacional

El uso de la Internet y el impacto que produce en los sistemas de información y de administración, así como la convergencia de componentes, computadoras, telecomunicaciones y electrónica, bases de datos acumulados y estructuras complejas de información, logran la necesidad de la existencia de una protección penal capaz de prevenir el mal uso de los sistemas informáticos en donde quiera que estos se desarrollen con el fin de crear mecanismos para la comisión de ilícitos. Estas consideraciones sentaron las bases para realizar una regulación específica en el derecho penal guatemalteco, por lo cual se plasma el Decreto 33-96 que se adicionó al Código Penal, creando los siguientes tipos penales:

El artículo 274 inciso a) regula la **Destrucción de Registros Informáticos** que consiste en destruir, borrar o de alguna manera inutilizar los registros informáticos. La pena se eleva a un tercio cuando la información, objeto de delito, es necesaria para la presentación de un servicio público o se trate de un registro oficial. [122]

El autor Miguel López Muñiz, citado por Lucerito Flores Salgado, señala que la división registral, en la informática, ocupa de todos los registros públicos, sean públicos o privados.[123] La comisión de este delito; vendría a ser consistente en la destrucción material, de cualquier modo, de registros electrónicos, causada por el sujeto activo que realizó las conductas idóneas para producir una afectación sobre el bien jurídico tutelado.

---

[122] Congreso de la República de Guatemala. Decreto 17-73. Código Penal. Artículo 274 "A"

[123] Flores Salgado, Lucerito. *Óp. Cit.* Página 67

En el mismo artículo 274, en el inciso b) se estipula la **Alteración de programas** que consiste en alterar, borrar o de algún modo inutilizar las instrucciones o programas que utilizan las computadoras.[124]

La **Reproducción de instrucciones o programas de computación (artículo 274 "C"):** El delito consiste en atentar contra el sistema de computación de alguna manera reproduciendo o copiando sus programas sin autorización del autor, normado en el inciso c) del artículo 274 del Código Penal. [125]

Es de hacer mención que el delito tiene relación estrecha con el delito de violación a los derechos de autor, pero enfocado con la protección en el ámbito informático buscando de esta forma la protección de bienes jurídicos tutelados de carácter patrimonial, así como el reconocimiento de la calidad de autor o inventor de instrucciones o programas informáticos. [126]

Para Flores Salgado, el software es un bien inmaterial que es objeto de derechos de propiedad intelectual que requiere la protección por parte de la ley, de esta forma, se establece un ámbito de protección que recae tanto sobre los programas de ordenador, definidos como aquellas secuencias o indicaciones destinadas a ser utilizadas en un sistema informático para realizar una función y obtener un resultado determinado. [127] La imputación de este tipo penal debe referirse a modo tiempo haciendo referencia al momento en que se copiaron o reprodujeron los programas, el autor del delito, y medios empleados para el desarrollo del delito.

El delito de **Registros prohibidos** implica la creación de una base de datos que pueda afectar la intimidad de las personas. La conducta se perfecciona al crear un

[124] Congreso de la República de Guatemala. Decreto 17-73. Código Penal. Artículo 274 "B"
[125] Ibíd. Artículo 274 "C"
[126] Ibíd. Artículo 274 "C"
[127] Flores Salgado, Lucerito. *Óp. Cit.* Página 97

banco de datos o un registro informático con datos que pudieran afectar la privacidad de los individuos. Esta figura se encuentra establecida en el artículo 274 inciso d) del Código Penal. **[128]**

De acuerdo con Noriega Salazar, el tenor del análisis de este artículo debe tomarse en cuenta que los datos de registro deben ser íntimos y de esa cuenta vale la pena profundizar sobre el ámbito de lo que debe entenderse como tal para diferenciarlo de lo privado.[129] Desde un punto de vista constitucional, acorde a lo estipulado en la Constitución Política de la República de Guatemala, existe una relación de la regulación de este tipo penal y la protección constitucional en cuanto a la dignidad, la integridad y la intimidad de los individuos.

La **Manipulación de información** consiste en el uso de registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación, o para ocultar, falsear o alterar estados contables o la situación patrimonio de una persona física o jurídica, se regula en el inciso e) del artículo y cuerpo legal ya mencionado. **[130]**

Al existir alteración de información, se hace referencia de manipular lo que es verdadero o de otro modo hacer una falsificación, entendiéndose esto como algo que no es auténtico. Alvarado y Morales refieren este supuesto de falsedad mediante la configuración de: la simulación, entendiéndose como una sustitución total de lo verdadero; y, mediante la alteración, cuando se modifica o cambia la esencia o forma de algo, o sea una sustitución parcial de lo verdadero.[131]

Relacionado a ello, el Código Penal tipifica el delito denominado como «Falsedad Material» en el artículo 321, el cual establece: «*Quien hiciere, en todo o en parte,*

[128] Congreso de la República de Guatemala. Decreto 17-73. Código Penal. Artículo 274 "D"
[129] Noriega Salazar, Hans Aarón. *Óp. Cit.* Página 42
[130] Congreso de la República de Guatemala. Decreto 17-73. Código Penal. Artículo 274 "E"
[131] Alvarado, Rolando y Ronald Morales. *Óp. Cit.* Página 91

un documento público falso, o alterare uno verdadero, de modo que pueda resultar perjuicio, será sancionado con prisión de dos a seis años».[132] Esto en materia informática haría referencia a los documentos públicos electrónicos entendiéndose como sujeto activo, quien tenga los conocimientos pertinentes para llevar a cabo la acción delictiva y el sujeto pasivo, lo constituye entonces el bien que se encuentra en riesgo afectando el patrimonio como consecuencia de estos actos.

El **Uso de información** se señala en el inciso f) del mismo artículo y cuerpo legal citado en donde se establece que existe la comisión del delito cuando quien sin autorización utiliza los registros informáticos de otro o ingresare, por cualquier medio, a su base de datos o archivos electrónicos. [133]

El delito correspondiente a los **Programas destructivos** se refiere a la distribución o circulación de programas o instrucciones destructivas, que puedan causar perjuicio a los registros, programas o equipos de computación; el cual está regulado en el artículo 274 inciso g) del Código Penal. [134]

En contexto con el tema relacionado en el presente trabajo de investigación, la Deep Web cuenta con una amplitud generada para el desarrollo de ilícitos; en esta plataforma pueden existir diversos mecanismos para la creación de delitos informáticos u otras actividades que generen a largo plazo el surgimiento de otros. La legislación guatemalteca tipifica como ilícitas otras conductas en las que podrían subsumirse actos que se desarrollan en la Internet Profunda. Entre las que se pueden mencionar:

[132] Congreso de la República de Guatemala. Decreto 17-73. Código Penal. Artículo 321
[133] Ibíd. Artículo 274 "F"
[134] Ibíd. Artículo 274 "G"

4.1.1 Violación a Derechos de Autor contenida en el artículo 274 del Código Penal.

Según Noriega Salazar, las obras producto del intelecto y los derechos sobre estas pueden encontrar vulneración a través del uso de las computadoras ya sea para reproducirlas, atribuirse falsamente su autoría, modificarlas o usarlas sin pagar los respectivos derechos.[135] En el área práctica se puede percibir por medio de la observación que la distribución de contenido por medio de archivos compactos tiene un fin lucrativo. Esto lo determina el artículo 274 al establecer que quien comete esta acción delictiva lo hace por medio de:

1. La reproducción de una obra, interpretación o ejecución, fonograma o difusión sin la autorización del autor o titular del derecho correspondiente.[136]

2. La adaptación, arreglo o transformación de todo o parte de una obra protegida sin la autorización del autor o del titular del derecho;[137]

3. La comunicación al público por cualquier medio o proceso de una obra protegida o de un fonograma sin la autorización del titular del derecho correspondiente.[138]

4. La distribución no autorizada de reproducciones de todo o parte de una obra o fonograma por medio de su venta, arrendamiento de largo plazo, arrendamiento, arrendamiento con opción a compre, préstamo o cualquier otra modalidad. [139]

[135] Noriega Salazar, Hans Aarón. *Óp. Cit.* Página 37
[136] Congreso de la República de Guatemala. Código Penal. Decreto 17-73. Artículo 274 c)
[137] Ibíd. Artículo 274 d)
[138] Ibíd. Artículo 274 e)
[139] Ibíd. Artículo 274 f)

5. La fijación, reproducción o retransmisión de una difusión transmitida por satélite, radio, hilo o cable, fibra óptica o cualquier otro medio sin la autorización del titular del derecho;[140]

6. Manufacturar, ensamblar, modificar, importar, exportar, vender, arrendar o de cualquier forma distribuir un dispositivo o sistema tangible o intangible, sabiendo o teniendo razón para saber que el dispositivo o sistema sirve o asiste principalmente para decodificar una señal de satélite codificada, que tenga un programa sin la autorización del distribuidor legal de dicha señal, o la recepción y distribución intencionada de una señal que lleva un programa que se originó como señal satelital codificada sabiendo que fue decodificada sin la autorización del distribuidor legal de la señal.[141]

7. Con respecto a las medidas tecnológicas efectivas lo siguiente: acto que eluda o intente eludir una medida tecnológica efectiva que impida o controle el acceso o el uso no autorizado a toda obra, interpretación o ejecución o fonograma protegido. [142]

Los incisos del citado artículo que fueron mencionados anteriormente entran en la temática directa de la actividad desarrollada en la Internet Profunda, lo cual fundamentalmente se alude de esta forma por el análisis de los supuestos que señala el legislador al desarrollar lo referente a la violación de los derechos de autor. De acuerdo con Juan Antonio Llobet Colom, el espíritu de la norma va dirigido a proteger el derecho al reconocimiento por la producción de una obra de cualquier tipo, que viene a ser el bien jurídico tutelado. La obra es fruto de la íntima concepción del ser inteligente quien, al combinar los elementos facilitados por el fondo común de las ideas, concibe y produce una obra original.[143]

---

[140] Ibíd. Artículo 274 h)
[141] Ibíd. Artículo 274 k)
[142] Ibíd. Artículo 274 l)
[143] Llobet Colom, Juan Antonio. *El Derecho de Autor, la legislación de Centroamérica y Panamá*. Guatemala. Editorial Piedra Santa. Pág. 3

Además Llobet Colom expresa, que el derecho de autor por sus características es un derecho inclasificable dentro de los derechos reales, pese a que entra en la esfera de los derechos patrimoniales pues no es de naturaleza personal exclusivamente. Constituye una disciplina jurídica "sui géneris"[144], (que significa de su propio género o especie). Los derechos de autor están relacionados a derecho moral que va de la mano con el acto creativo de la obra concebida. En ese sentido una investigación que la sustente debe ir dirigida a demostrar no solamente la vulneración al derecho reconocido por la ley sino también la afectación al patrimonio del autor legítimo por la susceptibilidad a perder ingresos netos por la distribución no autorizada de su obra.

La fundamentación legal es además proporcionada por el artículo 18 de la Ley de Derechos de autor y Conexos de Guatemala que señala: «*El derecho de autor comprende los derechos morales y patrimoniales que protegen la integridad, la paternidad y el aprovechamiento de la obra*».[145]

4.1.2 Violación a los Derechos de Propiedad Industrial contenida en el artículo 275 del Código Penal.

Para Rodrigo Bercovitz Rodríguez Cano la *Propiedad Industrial* es un conjunto de disposiciones cuyo objeto es la protección de las creaciones que tiene aplicación en el campo de la industria y el comercio y la protección contra la competencia desleal, incluyendo aquellos actos que infringen los llamados secretos industriales o secretos empresariales."[146] Ésta siempre tendrá como objeto la libertad de hacer uso exclusivo a las creaciones del autor siempre y cuando no haya un tercero que

[144] Loc. Cit.
[145] Congreso de la República de Guatemala. *Ley de Derechos de Autor y Derechos Conexos.* Decreto 33-98. Artículo 18
[146] Rodríguez Cano, Rodrigo Bercovitz et. al. Manual de Propiedad Intelectual. España. Editorial Tirant Lo Blanch. 2004. 4ta. Edición. Pág. 25

se encargue de difundir la creación haciéndose acreedor o titular de dicha obra, hacer plagio.

Como bien se puede mencionar Rodríguez Cano expresa hay determinadas restricciones al respecto de donde se puede difundir las creaciones y esto se refiere a los límites territoriales en donde puede ser difundida y estas son las que establece la *Propiedad Industrial,* así como la duración y validez que cierta obra debe tener en determinado territorio.[147]

4.1.3 Violación a la intimidad sexual contenida en el artículo 190 del Código Penal.

De acuerdo con Noriega Salazar, el término «*indemnidad sexual está relacionado directamente al libre desarrollo de la sexualidad, es la seguridad y protección que deben tener todos en el ámbito sexual para contar con la capacidad de reflexión y decisión*»[148]; lo cual da a entender, que se hace referencia a aquellas personas que no han llegado a un estado de madurez adecuado para contemplar el desarrollo de mantener relaciones de índole sexual, y ligado a este antecedente es el Estado quien debe velar por la protección de los menores de edad.

Este tipo penal está contenido en el artículo 190 del Código Penal, el cual marca dos modalidades: La primera consistente en la realización del acto por una persona a través de cualquier medio, sin el consentimiento de la víctima, lo cual atenta contra su intimidad sexual y a esa cuenta se apodere o capte mensajes, conversaciones, comunicaciones, sonidos, imágenes de su cuerpo para afectar su dignidad.[149] Noriega Salazar asevera que objetivamente la imputación del delito debe estar enfocada a partir de:[150]

---

[147] Loc. Cit.
[148] Noriega Salazar, Hans Aarón. *Óp. Cit.* Página 44
[149] Congreso de la República. Código Penal. Decreto 17-73. Artículo 190
[150] Noriega Salazar. Hans Aarón. *Óp. Cit.* Página 46

1) Que el sujeto activo de este ilícito realizó cualquiera de las acciones contenidas en los verbos rectores apoderar o captar.
2) Que estas acciones se realizaron sin el consentimiento del sujeto pasivo y atentando en contra de su intimidad, ejemplo la persona que espía, filma o fotografía a alguien que se está bañando desnudo o teniendo relaciones sexuales.
3) Con una intencionalidad concreta que es afectar su dignidad.
4) Que se realizó la difusión a terceros del producto de esa intromisión a la intimidad de la persona.

La segunda modalidad contenida en el artículo 190 del Código Penal se determina a la no autorización de apoderarse, acceder, utilizar, o modificar en perjuicio de tercero, comunicaciones o datos reservados de contenido sexual o familiar que se encuentren registrados en archivos informáticos o de otro tipo.[151] En los dos casos se agrava la pena cuando estas imágenes se hacen públicas y por lo tanto de fácil acceso. La Internet Profunda, aunque no es un sitio al que cualquier usuario de Internet pueda acceder fácilmente, logra difundir a manera integral la distribución de contenido que viole la indemnidad sexual de menores y otras personas para aquellos usuarios que logran sobrepasar las limitantes que restringen en cierto modo su acceso.

De lo anterior, se puede estipular que las proliferaciones en Internet de imágenes de contenido erótico atentan contra la intimidad sexual de los individuos y a esa cuenta el legislador ve la necesidad de crear una normativa que se encargue de prohibir cualquier tipo de conducta que genera acciones ilícitas de índole sexual. que atentaban contra la intimidad sexual de algunas señoritas, de esa cuenta el legislador determinó la necesidad de prohibir estas conductas.

De acuerdo con De Mata Vela y De León Velasco, *«el derecho de la intimidad sexual está integrado por un conjunto de elementos cuyo fin es proteger el derecho a*

[151] Congreso de la República. Código Penal. Decreto 17-73. Artículo 190 segundo párrafo.

conservar la vida privada dentro de la esfera personal, como un atributo de la vida familiar y personal.»[152] Esto refiere al ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión que perjudique directamente su desarrollo integral y fuera de las violaciones a a la esfera de derechos.

4.1.4 Producción de pornografía de personas menores de edad contenida en el artículo 194 del Código Penal; y la Comercialización o difusión de pornografía de personas menores de edad contenida en el artículo 195 Bis

Existe una importancia fundamental en la tipificación de las conductas que conllevan a la creación de contenido denominado como pornografía y en esta situación se convierte en un medio en el cual se ven involucrados menores de edad o personas que son incapaces de voluntad o conocimiento sobre los actos que envuelven este tipo de contenidos. La Internet Profunda en los últimos años ha servido como medio para realizar la producción y distribución de material altamente pornográfico que, por su naturaleza, es un delito de índole sexual donde se viola la indemnidad sexual de la persona.

El Código Penal en el artículo 194 se señala que: «*Quien de cualquier forma y a través de cualquier medio, produzca, fabrique o elabore material pornográfico que contenga imagen o voz real o simulada, de una o varias personas menores de edad o con incapacidad volitiva o cognitiva, en acciones pornográficas o eróticas, será sancionado con prisión de seis a diez años y multa de cincuenta mil a mil quinientos mil quetzales.»*[153]

Para Noriega Salazar, la acusación de este tipo de ilícitos como mínimo debe ir encaminada entonces a demostrar que el sujeto activo realizó:[154]

[152] De Mata Vela, José Francisco y Héctor Aníbal De León Velasco. *Óp. Cit.* Página 397
[153] Congreso de la República de Guatemala. Código Penal. Decreto 17-73. Artículo 194
[154] Noriega Salazar, Hans Aarón. *Óp. Cit.* Página 47

1. Cualquiera de las acciones descritas en los verbos rectores anteriormente mencionados.
2. Que el material pornográfico incluye imágenes o voces reales o simuladas de personas menores de edad o con incapacidad mental o cognitiva.

En efecto, agrega De Mata Vela y De Léon, el ente encargado de la persecución penal de individualizar las conductas que logran la distribución de pornografía infantil, remarcando que un delito sexual no conlleva con anormalidades, aberraciones o desviaciones sexuales.[155] Esto atiende además a lo preceptuado por la Declaración de los Derechos del Niño que en el Principio IX establece la importancia que tiene el niño de ser protegido contra toda forma de abandono, crueldad y explotación. No debe ser objeto de ningún tipo de trata.[156]

4.1.5 Comercialización de Datos Personales ilícito penal contenido en la Ley de Acceso a la Información Pública, artículo 64.

El artículo 64 del Decreto 57-2008 del Congreso de la República consistente en la Ley de Acceso a la Información Pública establece; «*Quien comercialice o distribuya por cualquier medio, archivos de información de datos personales, datos sensibles o personales sensibles, protegidos por la presente ley sin contar con la autorización expresa por escrito del titular de los mismos y que no provengan de registros públicos, será sancionado con prisión de cinco a ocho años y multa de cincuenta mil a cien mil Quetzales y el comiso de los objetos instrumentos del delito.»*[157]

El legislador en el citado artículo, refiere a los datos que se consideran de carácter sensible de una persona puesto que contiene material que índole personal y privada

[155] De Mata Vela, José Francisco y Héctor Aníbal De León Velasco. *Óp. Cit.* Página 384
[156] Asamblea General de las Naciones Unidas. *Declaración de los Derechos del Niño.* 1959. Principio IX.
[157] Congreso de la República de Guatemala. Ley de Acceso a la Información Pública. Decreto 57-2008. Artículo 64

para el afectado. De esta manera, existiría una violación hacia su vida privada, y en ese orden de ideas los elementos a ser probados refieren a la actividad de uno más individuos en conjunto que tienen como fin el comercio y/o distribución de material cuyo contenido signifique poner en riesgo la integridad y seguridad personal de uno o más individuos y el fomento de ganancias de ingresos monetarios a partir de las operaciones de compra y venta de este tipo de contenido.

4.2 Protección Jurídica Informática en el Derecho Convencional

Desde el ámbito del Derecho informático se ha orientado la necesidad por la creación de soluciones adecuadas a la problemática por el impacto de la informática en la sociedad actual. El Internet se ha convertido en la herramienta de primera necesidad en las comunidades alrededor del mundo y esto ha conllevado a la creación a nivel internacional de vínculos jurídicos que buscan una regulación a todo el movimiento que ha sido posible realizar a través de la progresión que tiene el fenómeno de la Internet.

Cabe mencionar, que a través de esta progresión es posible abrir una brecha en los sistemas de información que a la larga han conllevado a través del pasar del tiempo el surgimiento de plataformas virtuales capaces de lograr cualquier interés de los usuarios. Por su naturaleza la Deep Web no es la excepción, su existencia ha significado la obtención de una cantidad desmesurada de información cuyo propósito va desde perjudicar los derechos de los individuos hasta el acceso a contenido, que tiene suma importancia para los usuarios y Estados alrededor del mundo, que no tienen un fin dañino hacia la sociedad.

De acuerdo con Téllez Valdes las áreas generales de injerencia de las computadoras a nivel de transferencia de información, uso institucional y privado para fines de gestión y aun a nivel sociocultural, el desarrollo de la computación ha permitido un sinnúmero de avances que se reflejan en los siguientes ámbitos:[158]

[158] Téllez Valdes, Julio. *Óp. Cit.* Página 16-17

a) Las oficinas y el surgimiento de la ofimática.
b) Gerencial, con una adecuada formulación de políticas, planeación y conducción de estrategias de organización
c) Supervisión y control, con una mejor comunicación, dirección y vigilancia de empleados.
d) Administración, con un adecuado control de nóminas, contabilidad, inventarios.
e) Industrial y el surgimiento de la robótica que ha permitido un aumento en la productividad de las fábricas con reducciones de tiempo y costos.
f) Bancario, con sistemas de pago automatizado, autorización de crédito, transferencia de fondos, asesorías financieras.
g) Salud, con una mejor preparación de historias clínicas, exámenes y diagnósticos más completos.
h) Hogar, con una adecuada administración de presupuesto, control de uso de energía, análisis de inversión y preparación de la declaración de impuestos.

Dichas áreas componen una gama amplia en donde el acceso de las tecnologías e Internet han tenido un impacto significativo para las personas puesto que facilitan en gran manera el estilo de vida actual. En años recientes han surgido cambios drásticos en el funcionamiento, estructura y aplicación de las computadoras.

Esto ha permitido la facilidad de transmisión de datos para desarrollar los avances tecnológicos que permiten el desarrollo en la sociedad. Esto va de la mano con la importancia en el reconocimiento de la intimidad o vida privada de los individuos, así como los bienes que son susceptibles a una tutela jurídica. La informática y sus instrumentos ciertamente han permitido, para Altmark y Molina Quiroga, la creación de grandes bancos de datos que permiten una gran concentración de enormes

volúmenes de información de carácter personal, con la suma de la estructuración de sistemas que garantizan su rápida y eficiente recuperación.[159]

El desarrollo del Derecho Informática, por ser una de las ramas del conocimiento jurídico más nuevas, a comparación del derecho convencional a lo largo de la historia del ser humano, se encuentra en continuo desarrollo teniendo en los años recientes sus incipientes significativos en la sociedad. La época de las telecomunicaciones genera fenómenos sociales que tienen significancia para el derecho y a partir de ello es posible brindar una protección jurídica a los derechos adquiridos desde la creación de los primeros ordenadores.

Téllez Valdés manifiesta «*Esta susceptibilidad para la aplicación del derecho es inminente pues se ha manifestado como un régimen regulador de intereses particulares y colectivos».* [160] Es menester que, en esta materia, los datos personales de los usuarios deben contar con dicha protección jurídica para salvaguardar la integridad de los individuos que tienen en un constante o casual acceso a las redes informáticas.

La *Deep Web* o Internet Profunda entre sus fines, como se ha mencionado anteriormente, es un espacio creado para la exclusividad de manejo de información sin tener un apego regulatorio legal por parte de algún Estado, lo cual ha generado que esta se haya convertido en un medio facilitador para el desarrollo de actos que en su mayoría van en contra de lo preceptuado por las doctrinas legales y regulaciones estatales. Citando a Altmark y Molina Quiroga, *«con la informática y las telecomunicaciones no se descubre la preocupación del derecho a la intimidad, pero es evidente que el portentoso aporte de la tecnología requiere, a efectos de proteger adecuadamente los derechos del individuo de una normativa…»*[161]

[159] Altmark, Daniel Ricardo y Eduardo Molina Quiroga. *Informática y Derecho. Aportes de Doctrina Internacional*. Volumen VI. Argentina. Ediciones Depalma. 1998. Página 146
[160] Téllez Váldes. Julio. *Óp. Cit.* Página 20
[161] Altmark, Daniel Ricardo y Eduardo Molina Quiroga. *Óp. Cit.* Página 146 y 147

Es por ello, que las normativas que deben ser creadas por los Estados en virtud de la protección de los derechos del individuo deben estructurar una metodología que efectivamente haga frente a los riesgos que surgen a partir del uso de las tecnologías. El derecho constituye, para Noriega Salazar, una materia en extremo cambiante, que evoluciona y se desarrolla de la mano con las transformaciones y necesidades de la sociedad.[162] Como conveniencia, para los avances de las civilizaciones han creado la necesidad de regular por parte de normas legales aspectos y bienes jurídicos.

Relacionado con lo anterior, el Derecho Penal, constituye un papel importante en la evolución de los sistemas de información puesto que existe la necesidad de regular los ámbitos de protección para los bienes jurídicos tutelados que hoy en día deben ser merecedores de una defensa por parte de los Estados.

4.2.1 Protección Jurídica de los Datos Personales e Intimidad Personal de los Usuarios de Internet

La protección jurídica hacia los datos personales e integridad personal es una institución que debe ser reconocida en todos los Estados a nivel mundial, puesto que se trata de ámbitos que recaen en los derechos inherentes de todos los individuos. Fundamentalmente esta protección debe ir encaminada en los aspectos que compatibilizan la normativa adecuada para garantizar que estos derechos no sean vulnerados y tengan una incidencia negativa en la sociedad.

Flores Salgado, determina este ámbito como el derecho a la intimidad, el cual consiste en «*dotar a las personas de cobertura jurídica frente al peligro que supone la informatización de sus datos personales.»* [163] De esta forma, el principio fundamental para la protección de la integridad tendría una intromisión en la esfera

[162] Noriega Salazar, Hans Aarón. *Óp. Cit.* Página 21
[163] Flores Salgado, Lucerito. *Óp. Cit.* Página 89

de derechos que los individuos que permitiría dejar a un lado la vulneración de su integridad.

Flores Salgado asevera que la noción de intimidad es acuñada por el vocablo *privacy* que la conceptualiza como aquella consistente en la esfera íntima que comprende hechos de la esfera de la libertad de la autodeterminación de la personalidad, así como la protección de datos computarizados que no sean de dominio público.[164] Ello se entiende como aquella parte del individuo que no está consagrada hacia una actividad de índole público, en donde los terceros no tendrían que tener una injerencia. La protección de datos conlleva a respetar la intimidad de las personas.

Las bases de datos pueden ser de carácter público o privado y estos deben considerar el salvaguardar la integridad de la persona cuyos datos personales son administrados en alguna base. La Deep Web genera una base de datos e información filtrada por otros usuarios para conllevar actos ilícitos que atentan contra los derechos personales de los individuos, y que por su naturaleza, la libertad y anonimato que la caracteriza permite la realización de actividad que genera la transfusión de datos a través de las fronteras virtuales.

Es por ello, que la protección de los datos personales se ubica en un campo de derecho informático, ya que debe ser una garantía o facultad de control de la información frente al tratamiento que las tecnologías ofrecen hacia los usuarios de Internet. Los derechos personales de los individuos pueden verse vulnerados en el tráfico de datos que es posible en la Internet; su protección es indispensable para garantizar el bienestar personales de los usuarios, ya que eso conllevaría el respeto y la navegación segura en los sitios virtuales en cualquiera de sus plataformas.

[164] Ibíd. Página 90.

4.2.2 Protección Jurídica de los Programas de Computación y Ordenadores

Téllez Valdes enuncia que «*el problema de la protección de los programas de computación no es estrictamente jurídico, sino que denota la presencia de dos elementos fundamentales como lo son el técnico y el económico.»*[165] En ese orden de ideas, el ámbito jurídico entraría en una etapa secundaria en cuanto protección que se le debe brindar a los programas de computación y ordenadores puesto que existen circunstancias que deben ser ventiladas desde un punto de vista técnico y económico.

El ámbito técnico, según Téllez Valdes, partiría desde el punto de clasificar a los programas de cómputo como el conjunto de procedimientos o reglas que integran el soporte lógico de las máquinas y que permiten la consecución de tratamiento de información. [166] Los programas están relacionados de manera concreta con los lenguajes de programación que forman una cadena de enlace entre la interacción del usuario hacia el lenguaje del ordenador. Los dispositivos electrónicos deben tener un medio de protección de alcance y eficacia para proporcionar seguridad sus programas e información contenida en ellos.

Además, en esa misma línea Téllez Valdes afirma que el ámbito económico genera una importancia que reviste el bienestar de la información virtual; puesto que los programas de computación son una de las máximas manifestaciones del producto de información que han provocado el apuntalamiento de la industria de la programación, lo que trae consigo que los problemas en torno al ordenador alcancen un nivel económico y, por ende, jurídico.[167] Los ataques informáticos que buscan primordialmente los sistemas de información y cómputo han llevado a los usuarios a mantener un estándar de vigilancia y constante precaución hacia los percances económicos que conllevan éstos.

---

[165] Téllez Valdes, Julio. *Óp. Cit.* Página 85
[166] Ibíd. Página 86.
[167] Loc. Cit.

Es por ello, que el *software,* es un bien inmaterial objeto de derechos de propiedad intelectual, requiriendo por parte de la normativa legal, la garantía para su protección. De acuerdo con Antonio Pérez Luño, citado por Flores Salgado, la protección jurídica de los programas es por parte de:[168]

a) La empresa que se dedica a la elaboración de programas y que busca defender sus invenciones, considerando la fuerte inversión en investigación y elaboración.
b) Del programador o programadores para que se les reconozca la "nula paternidad" del programa a efectos de su promoción profesional, aunque la empresa tenga los derechos de explotación.
c) Interés genérico en el avance de la investigación, ya que cuando se da a conocer la protección de un programa se evita su repetición.

El *software* debe contar con mecanismos de protección mediante los cuales permitan su seguridad jurídica, y partir de esta idea el derecho debe ir encaminado a velar por la creación de instrumentos de protección mediante las vías jurídicas. Téllez Valdes respecto a ello señala que, en la vía civil, esta protección se realiza por medio de los contratos y mediante el conjunto de cláusulas introducidas en él y alusivas a la seguridad y protección de los programas, consignado el eventual acceso a los mismos por personas no autorizadas, uso inadecuado, modificaciones no pactadas, destrucción de la información, etc.[169]

[168] Flores Salgado, Lucerito. *Óp. Cit.* Página 97.
[169] Ibíd. Página 98

CAPÍTULO 5

Casos relacionados a la Internet Profunda y Delitos Informáticos

En cuanto la comprensión de los límites existentes entre los derechos de libertad de expresión y de acceso información, se desarrollan a continuación casos en los cuales la Internet Profunda o *Deep Web,* tanto en relación con los delitos informáticos, se ha visto implicada directa o indirectamente.

5.1 *Silk Road*

En concordancia a los hechos que conforman el modelo de negocio de los grandes cárteles de drogas ha implicado la necesidad de protección armada con otros criminales. Los delitos violentos y el tráfico de drogas representan amenazas serias para el Estado de Derecho y el desarrollo en Centroamérica y el Caribe. De acuerdo con declaraciones del Director Ejecutivo de UNODC, Yury Fedotov, «*la relación entre el desarrollo, el Estado de Derecho y la seguridad necesita ser totalmente comprendida. Las drogas y el delito son también problemáticas vinculadas con el desarrollo, mientras que la estabilidad puede promoverse a través de la adopción de los derechos humanos y el acceso a la justicia*».[170]

De acuerdo a ello, el hecho de adquirir drogas tiene distinta relevancia penal en los distintos países. Las legislaciones de distintos países catalogan el delito en cuanto a la tenencia de drogas, adquisición, consumo, etc. Esto hace que el pequeño comprador, que busca simplemente un abastecimiento para su propio uso, tenga que verse negociando con personajes que pueden reaccionar de forma violenta.

De acuerdo con la entidad *Bitcoin*, la explosión de los mercados anónimos de drogas que hizo posible *Bitcoin* y *Tor* en la *Deep Web* está asentándose como paradigma en un nuevo mercado que ya no necesita de la presencia real. Por una

[170] Oficina de las Naciones Unidas contra la Droga y el Delito. UNODC. *Tráfico de Drogas en Centroamérica y el Caribe.* Austria. 2014. Disponibilidad y acceso en: https://www.unodc.org/ropan/es/BorderControl/drug-trafficking.html Fecha de consulta 25/03/2017

parte, el mercado negro tradicional que ofrece la posibilidad de comprobar aquello por lo que se paga en el mismo momento en que se entrega el dinero.[171] *Silk Road* o *Ruta de Seda* surge en febrero del 2011 como un lugar de encuentro online para la compraventa de artículos prohibidos. El ofrecimiento entre sus productos contenía principalmente drogas ilegales tales como marihuana, opiáceos, alucinógenos, benzodiacepinas, éxtasis entre otras.[172]

Nicholas Christin, investigador de la universidad Carnegie Mellon ubicada en Pennsylvania, Estados Unidos de Norte América, realizó un estudio en cuanto su funcionamiento durante seis meses publicó sus conclusiones, estableciendo que el volumen de negocio realizado en el sitio web superaba los 22 millones de dólares al año.[173] Además programó un sistema que visitaba la web a diario para recopilar datos. Su software registraba y catalogaba de manera automática los nuevos productos a la venta, los vendedores y las valoraciones de los compradores.

Esta tienda virtual de estupefaciente estuvo diseñada, principalmente, para garantizar el anonimato, tanto de los compradores como vendedores, para generar un grado de confianza y seguridad entre ellos. *Silk Road,* de esta forma se convirtió en un intermediario anónimo entre dos. Según el estudio realizado por Christin, los artículos más requeridos fueron el cannabis y sus derivados. Durante el periodo de la investigación se ofertaron más de 4.000 dosis entre marihuana, hachís y otros. Un 20,7 por ciento del total. Otros productos de «éxito» fueron los medicamentos

[171] BITCOIN. *Silk Road como herramienta para reducir la violencia.* Estados Unidos. 2016. Disponibilidad y acceso en: http://elbitcoin.org/silk-road-como-herramienta-para-reducir-la-violencia-en-los-mercados-de-drogas/ Fecha de consulta 24/03/2017

[172] La Penúltima. *Silk Road: El tráfico de drogas abre su tienda en internet.* España. 2012. Disponibilidad y acceso en: http://lapenultima.org/silk-road Fecha de consulta 24/03/2017

[173] Cornell University Library. Nicholas Christin. *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace.* Estados Unidos. 2012. Disponibilidad y acceso en: https://arxiv.org/abs/1207.7139 Fecha de consulta 24/03/2017

que exigen receta (7,3% del total) y las benzodiacepinas (tranquilizantes como el Valium, que casi alcanzaron el 5%).[174]

De acuerdo con lo anterior, *Silk Road* se colocó no solamente como un mercado de productos prohibidos, sino también en una tienda para los defensores del anonimato y el cifrado de datos como garantía de la libertad individual, así como lo señala Piciarelli acerca sobre la proliferación de las actividades ilícitas. [175] Tal y como la creación de la *Deep Web* y sus orígenes la ideología conllevaba a la eliminación del Estado y una sociedad basada en la soberanía individual, la propiedad privada y el libre mercado; además del uso de *TOR* para evitar el rastreo de conexiones, los usuarios de *Silk Road* utilizaban el *bitcoin* como su divisa que les permitía realizar transacciones anónimas, como es detallada en el primer capítulo.

La Penúltima, como lo detalla en su artículo llamado *«Silk Road: El tráfico de drogas abre su tienda en internet», Silk Road* era un foro con el explícito propósito de reducir los daños de la guerra contra las drogas y facilitar el intercambio pacífico. El sitio contenía recomendaciones sobre el uso de las substancias, repartía agujas nuevas sin costo, y algunos vendedores se rehusaban a vender a gente que les parecía irresponsable.[176] Sin embargo, las investigaciones que realizaron las autoridades estadounidenses, luego de una extensiva búsqueda para determinar la ubicación e información relacionada con el administrador del sitio, lograron determinar con un joven llamado Ross Ubricht.

De acuerdo con el artículo citado en el párrafo anterior, la policía federal estadounidense arrestó a Ulbricht en octubre de 2013, acusándolo de ser *Dread*

---

[174] La Penúltima. *Silk Road: El tráfico de drogas abre su tienda en internet.* España. 2012. Disponibilidad y acceso en: http://lapenultima.org/silk-road Fecha de consulta 24/03/2017

[175] Almudi. Piciarelli, Fabrizio. *El «Deep Web»: el lado oscuro de Internet. Un viaje más allá de las fronteras de la red.* España. 2017. Disponible en: https://www.almudi.org/noticias-articulos-y-opinion/11416-el-deep-web-el-lado-oscuro-de-internet-un-viaje-mas-alla-de-las-fronteras-de-la-red Fecha de consulta: 21/04/2017

[176] Hempyreum. "*Deep Web" narra la historia del mártir de la guerra contra las drogas.* Suiza. 2015. Disponibilidad y acceso en: http://www.hempyreum.org/arc/es/71782 Fecha de Consulta 24/03/2017

Pirate Roberts, la mente detrás de la página web; en mayo de 2015, la jueza de Nueva York Katherine Forrest lo sentenció a cadena perpetua sin posibilidad de libertad condicional. Probablemente *Dread Pirate Roberts*, cuyo nombre viene de un personaje de ficción hayan sido distintos individuos entre 2011 y 2013. Aun así Ulbricht reconoció haber fundado el sitio a pesar de que eran varios los administradores que usaban la cuenta de *Dread Pirate Roberts*; así, el único acusado de operar Silk Road fue Ross Ulbricht.[177]

La Penúltima relata además que, inicialmente, la Fiscalía lo acusó de seis cargos, incluyendo asesinato y sicariato, para así negarle la posibilidad de fianza. Dos meses más tarde, la imputación definitiva solo fue por narcotráfico, conspiración para cometer delito informático y lavado de dinero. La propia Fiscalía reconoció que ninguna persona fue asesinada. Sin embargo, las acusaciones relacionadas con homicidios inexplicablemente quedaron en el expediente del juicio, lo cual habrá influenciado al jurado en la condena.[178]

Al tomar en cuenta la posición en la que se encontró Ulbricht al dictar la sentencia que lo condenó a cadena perpetua sentó una de las bases para la creación de sitios web en donde los criminales utilicen el *Bitcoin* como la moneda digital que permite el anonimato. En ese orden de ideas, puede decirse que él fue el responsable de abrir un mercado en la nube digital y en cierta forma demostró que existe una manera alternativa para el tráfico de drogas. Aunque es cierto que el modelo de *Silk Road* favorece las transacciones limpias, hay que decir que la violencia también cotiza en esos mercados, aunque sea violencia ejercida digitalmente. Este sitio permitió vislumbrar el futuro de la venta de drogas mientras no exista una opción regulada vía Estado.

La entidad *El Bitcoin* asegura que según expertos, se ha determinado que *Silk Road* fue efectivo reduciendo la violencia asociada a los mercados tradicionales de drogas, porque el vendedor no podrá atacar al comprador ni verse atacado lo que reduce la

[177] Loc. Cit.
[178] Loc. Cit.

necesidad de índice de violencia derivada de las malas leyes es una buena razón para darle una oportunidad a mercados como *Silk Road*.[179]

5.2 *Wikileaks*

WikiLeaks, tal y como lo detalla en su sitio web, es una organización mediática internacional sin ánimo de lucro que publica a través de su sitio web informes anónimos y documentos filtrados con contenido sensible en materia de interés público, preservando el anonimato de sus fuentes fundada por Julian Assange en 2006. WikiLeaks tiene relaciones contractuales y vías de comunicación seguras a más de 100 grandes organizaciones de medios de todo el mundo. Esto les da a las fuentes de WikiLeaks negociar el poder, el impacto y las protecciones técnicas que de otro modo serían difíciles o imposibles de lograr.[180]

Alberto Quian señala que "*la organización WikiLeaks ha ocupado portadas de periódicos y revistas de todo el mundo, ha abierto informativos de las principales cadenas de televisión, ha sido objeto de numerosos reportajes y documentales, y se ha propagado en Internet, además de generar una extensa colección de libros y guiones cinematográficos centrados en la figura de su enigmático fundador, el hacker australiano Julian Assange, y en el fenómeno de las filtraciones masivas de documentos secretos de gobiernos y corporaciones transnacionales.*"[181]

Quian expresa además que, WikiLeaks y su fundador alcanzaron notoriedad mundial en el año 2010 con una serie de filtraciones masivas de documentos secretos relacionados con las guerras de Irak y Afganistán, con las revelaciones del famoso caso *Cablegate* sobre los entresijos de la política exterior de Estados Unidos. Estos se hicieron públicos con la filtración de miles de cables diplomáticos

---

[179] BITCOIN. *Silk Road como herramienta para reducir la violencia.* Estados Unidos. 2016. Disponibilidad y acceso en: http://elbitcoin.org/silk-road-como-herramienta-para-reducir-la-violencia-en-los-mercados-de-drogas/ Fecha de consulta 24/03/2017

[180] Wikileaks. *What is Wikileaks.* Holanda. 2016. Disponibilidad y acceso en: https://wikileaks.org/What-is-Wikileaks.html Fecha de Consulta 26/03/2017

[181] Quian, Alberto. *El impacto mediático y político de Wikileaks: la historia más apasionante del periodismo moderno*. España. Editorial UOC. 2013. Página 9

entre el Pentágono y las embajadas estadounidenses repartidas por todo el mundo.[182]

Quian continuando con su estudio detalla que fue en esa época que las publicaciones ocasionaron un impacto mundial en las esferas de la políticas y los medios y generó controversia en cuanto a la determinación de las intenciones de su fundador, Julian Assange, y de su organización sobre la legitimidad de revelar secretos de Estado y corporativos, sobre la transparencia y el derecho a la información y a la libertad de expresión.[183] Por otro lado agrega, que su ideología se encontraba encaminada a filtrar masivamente los documentos secretos que poseía WikiLeaks para hacer famosa su organización y para lograr el máximo impacto político. Y esto solo era posible con el máximo impacto mediático.[184]

Esto impacta en la relación que tienen los gobiernos para buscar las vías directas para generar restricciones o presiones sobre las compañías con las que WikiLeaks sostiene su operación, de acuerdo al autor. Quian sostiene que en cuanto mayor fuese el acceso de WikiLeaks a los ciudadanos y su impacto en la opinión pública, mayor sería el impacto político. Este se alcanzaría mediante una cooperación sin precedentes entre cinco de las mayores organizaciones de noticias del mundo, que a la vez reportaron legitimidad y popularidad a WikiLeaks. Estas compañías son: *The New York Times* (Estados Unidos), *The Guardian* (Reino Unido), *Le Monde* (Francia) y *El País* (España), y el magazine *Der Spiegel* (Alemania).[185]

De acuerdo con lo publicado por la Organización de las Naciones Unidas en su artículo «*UN human rights chief voices concern at reported 'cyber war' aganist Wikileaks»,* la estrategia del máximo impacto mediático para conseguir el máximo impacto político obligó a WikiLeaks a renunciar a principios de la ética *hacker* y a acatar la función de *gatekeepers* de los periodistas y del propio gobierno de Estados Unidos. Este tipo de conductas motivaron un llamado de atención de la parte de la

[182] Loc. Cit.
[183] Ibíd. Página 10
[184] Ibíd. Página 115
[185] Ibíd. Página 116

alta comisionada de la Organización de las Naciones Unidas para los Derechos Humanos, Navi Pillay, quien consideró que «*si WikiLeaks ha cometido alguna ilegalidad, esta debería ser tratada mediante el sistema legal, y no mediante presiones o intimidaciones a terceras partes*.»[186]

Lo anterior obliga a poner en consideración principios del derecho internacional de los derechos humanos destinados a la libertad de expresión y el derecho a la información para dirimir qué conductas de WikiLeaks podrían ser efectivamente objeto de prohibición o sanción. Según los "Principios de Johannesburgo sobre Seguridad Nacional, Libertad de Expresión y acceso a la información", para que un Estado pueda tomar acciones para limitar la difusión de los contenidos de WikiLeaks debería mostrar:

1. Que esa posibilidad está prescrita en la ley.[187]
2. Que la información es de interés legítimo de seguridad nacional.[188]
3. Que tal información está prevista como susceptible de reserva por una autoridad superior y que esa decisión es revisable ante el tribunal independiente.[189]
4. Que la información es lesiva para el interés público.[190]

Según Quian, el medio es la demostración de poder de WikiLeaks como organización nómada, apátrida, transnacional y vinculada a la ética hacker que busca no solo subvertir la estructura tradicional de los poderes político y económico

---

[186] United Nations. *UN human rights chief voices concern at reported "cyber war" against WikiLeaks.* Estados Unidos. 2010. Disponibilidad y acceso en: http://www.un.org/apps/news/story.asp?NewsID=37009#.WOKEXNJrukp Fecha de Consulta 25/03/2017

[187] Centro contra la Censura y Centro de Estudios Legales Aplicados. Universidad de Witwatersrand, en Johannesburgo. *Los Principios de Johannesburgo sobre Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información.* Reino Unido. 1996. Disponibilidad y acceso en: https://www.article19.org/data/files/medialibrary/1803/Johannesburg-Principles.Spa.pdf Fecha de consulta: 25/03/2017 Principio 1.1

[188] Ibíd. Principio 2

[189] Ibíd. Principio 7

[190] Ibíd. Principio 13

y desmantelar el secreto como mecanismo de gobierno, control y manipulación que utilizan los Estados sino que además cuestiona el papel que los medios de información y los periodistas.[191]

5.3 *Anonymous*

De acuerdo con Morales y Alvarado, el término en inglés «*anonymus»* significa «*anónimo»,* y constituye un seudónimo utilizado a nivel mundial por un grupo indeterminado de personas que reciben ese nombre porque no revelan su identidad, y que como actividad principal es realizar ataques cibernéticos caracterizados por la libertad de expresión, independencia y su oposición a ciertas organizaciones, es decir, son anónimos. No existe una jerarquización entre sus miembros.[192] Principalmente, el grupo realiza sus acciones mediante ataques a sistemas de propiedad de los entes o personas que consideran adversarios.

Según Christopher Holloway, referido por Morales y Alvarado, «*el origen de Anonymous se puede rastrear hasta el sitio 4chan, que es básicamente una image board, un tipo de agregador de contenido en Internet que permite a sus usuarios crear y publicar temas de manera anónima anulando individualidades y dando paso a todo tipo de expresión, tanto creativa como violenta."*[193] A partir de ello se constituye su hegemonía para la creación del activismo *hacker*.

De acuerdo con Proyecto Idis, el activismo *hacker* es conocido como un fenómeno diferente al terrorismo cibernético que consiste en crear tecnología para conseguir un objetivo político o social en la red.[194] Por otra lado, Morales y Alvarado expresan que *Anonymous* es considerado como el grupo de hackers más célebre en la actualidad constituyéndose como un poder colectivo en donde entre sus miembros

[191] Quian, Alberto. *Óp. Cit.* Página 118
[192] Morales, Ronald y Rolando Alvarado. *Óp. Cit.* Página 187
[193] Ibíd. Página 189
[194] Proyecto Idis. *Activismo Hacker*. Canadà. 2013. Disponibilidad y acceso en: http://proyectoidis.org/activismo-hacker/ Fecha de consulta: 23/03/2017.

no existe jerarquía alguna. Al realizar sus ataques cibernéticos facilitan la infiltración a información cuyo propósito consistiría en perjudicar a los Estados.[195]

Morales y Alvarado señalan que los mecanismos de ataque de Anonymous consisten en el envío de un elevado número de peticiones a un servidor que aloja una página web, de tal forma que el servicio de almacenamiento web no puede soportar la carga de peticiones y suspende el servicio; este movimiento pretende rebasar la capacidad de volumen de datos que tiene el servidor de determinada organización. [196] Sus ataques cibernéticos tienen impacto mundial pues la vulnerabilidad de las páginas web de organizaciones y entidades permite que se desarrollen estos ataques.

En análisis de lo anterior da la pauta para establecer que este grupo de *hacktivistas*, por su concordancia al activismo *hacker*, cuenta con los medios y conocimientos necesarios para realizar sus actividades ilícitas como amenazas y ataques hacia aquellos sitios considerados como enemigos.

Según Morales y Alvarado entre sus ataques u operaciones más emblemáticas se puede mencionar la denominada *The Internet Strikes Back (Internet contraataca),* en la cual el Departamento de Estado de Estados Unidos de América en conjunto con la Oficina Federal de Investigación, FBI (por sus siglas en inglés), efectuaron una operación en contra de la conocida página web llamada «*Megaupload»*, cuya función principal consistía en el intercambio de archivos, resultando de esta forma su clausura. El caso con este sitio es la responsabilidad de sus directores, así como de las compañías vinculadas a ella para el desarrollo de la piratería masiva sobre diferentes obras protegidas, llegando a determinar que en materia de daños generados éstos ascendían a 500 millones de dólares. [197]

Claramente la existencia de violación de derechos de autor de dichas obras constituyó la persecución penal de los entes mencionados, ocasionando el cierre

[195] Morales, Ronald y Rolando Alvarado. *Óp. Cit.* Página 190
[196] Loc. Cit.
[197] Ibíd. Página 192 y 193

definitivo de dicho sitio web. En concordancia con lo anteriormente expuesto, el tipo de contenido abarcado en esta plataforma consistía en uno de los medios para la adquisición y tráfico de contenido ilícito, puesto que, no existía legalmente permiso de los autores para su difusión. *Megaupload* en cierto modo, contenía un vínculo con la Internet Profunda, por la vulneración sobre estos actos.

Morales y Alvarado continúan exponiendo que el papel de *Anonymous* recayó en los ataques que realizó a las entidades que consideró vinculadas a la denuncia e investigación del cierre de este sitio. Este ataque es considerado como *DdoS,* el cual consiste en la utilización de múltiples *hosts,* o servidores de transferencia de archivos, para lanzar un largo y coordinado ataque a una máquina, con el objeto de denegar el acceso o indisponer un sistema.[198] Los autores agregan que ello implicó a más de 27,000 ordenadores y cerca de 10,000 usuarios operando; significando de esta forma la catalogación de este ataque cibernético como el mayor de la historia. Fueron afectados el Departamento de Justicia, Oficina Federal de Copyright y la Jefatura de la Policía de Utah.[199]

[198] Ibíd. Página 82
[199] Ibíd. Página 193

CAPÍTULO 6

Presentación, Análisis y Discusión de Resultados.

La Deep Web o la Internet Profunda, como también se le conoce, es un espacio en la red que no puede pasar desapercibido por la regulación normativa de un Estado tomando en cuenta que existe una seria importancia de la creación y aplicación de legislación que proteja la integridad de los usuarios de internet.

En sí, al ser una plataforma que ofrece múltiples oportunidades a sus usuarios, también puede ser una vía para afectar los derechos de las personas. Esto ha impulsado la realización de actividades ilícitas, cuyos autores se encuentran al amparo de nuevas herramientas tecnológicas que facilitan el ejercicio de sus actividades delictivas. De alguna manera, se ha concebido una idea, que puede ser debatible, en donde hasta cierto punto la Deep Web es catalogada como un espacio totalmente peligroso y significativo para provocar un riesgo hacia los usuarios de Internet.

Por lo que se ha expuesto en lo párrafos anteriores, se infiere que puede ser utilizada como una herramienta que afecta derechos y garantías reconocidos en la ley, por individuos cuyos conocimientos son aplicados para la generación de actos ilícitos, aprovechando la ventaja de los espacios que sólo la Internet brinda para afectar la integridad de los usuarios. A partir de ello cabe de preguntar: ¿La Deep Web es indiscutiblemente un espacio exclusivo para la comisión de delitos?

Con base en la información previamente investigada y recopilada, con su respectivo análisis y confrontación de resultados con la doctrina y antecedentes del tema, el presente capítulo versará sobre los resultados que se obtuvieron en la investigación del campo en relación al tema. Se realizará el aporte jurídico a los presentes temas expuestos, para detallar de mejor manera el entorno de la situación jurídica en el que encaja la Deep Web, además de analizar el impacto que genera en la sociedad virtual la existencia de esta plataforma.

Para ello, se utilizó como instrumento de investigación: la entrevista.

6.1 Entrevistas

Para efectos de una recopilación de información más objetiva según los intereses de investigación se procedió a desarrollar dos tipos de entrevista: la primera, que estará enfocada en el ámbito jurídico y legal que se desenvuelve en la Deep Web y delitos informáticos, constando de nueve preguntas abiertas. Para el efecto, se dirigió la entrevista a las siguientes personas:

1. Lic. Carlos Alberto Solís Garza, ex catedrático de la Universidad Rafael Landívar del curso “Introducción a la Informática Jurídica”.
2. Lic. José Rolando Alvarado Lemus, co-autor del libro “Cibercrimen”.
3. Amílcar De León, Consultor en Seguridad Informática.

La segunda entrevista, estará enfocada en conocer desde un punto de vista técnico la experiencia de usuarios que han ingresado a esta plataforma, constando de cinco preguntas abiertas. Para el efecto se dirigió la entrevista a las siguientes personas:

1. Ingeniero Melinton Navas, analista en seguridad informática y catedrático de la Universidad del Valle de Guatemala.
2. Ingeniero Ronald Morales, co-autor del libro “Cibercrimen”.
3. Ingeniero Juan Pablo Barrera, de Pakal Security Labs.

6.1.1. Primer Modelo de Entrevista

Pregunta #1: ¿Qué importancia tiene la regulación de las actividades que se desarrollan en Internet?

Las personas entrevistadas concordaron en cuanto a reconocer la importancia vital para la regulación de las actividades desarrolladas en internet, especialmente en

materia de Comercio Electrónico y Cibercrimen como lo menciona Alvarado. Esto hace necesario propiciar la protección de derechos y obligaciones que surgen a través de las relaciones contractuales de los usuarios de internet, lo cual concuerda con lo descrito en los capítulos anteriores en relación a la libertad que permite la internet de poder desarrollar distintas actividades que estén enfocadas a cometer actos ilícitos.

Por otra parte, es importante mencionar que, aunque es complicada una regulación normativa concreta, significaría un gran avance para la legislación de los países de Latinoamérica y el Caribe, en donde la mayoría no cuenta con la regulación adecuada, la creación de normas que garanticen la certeza jurídica y seguridad de derechos de los usuarios de Internet, tal como lo comenta De León. Aplicado en Guatemala este principio de protección de derechos de las personas encuadra en lo establecido por el artículo 1 y 2 de la Constitución Política de la República.

Pregunta #2: ¿De qué manera considera que el internet ha significado una herramienta indiscutible para el desarrollo de muchos países, incluyendo a Guatemala, así como la facilidad para la elaboración de actividades ilícitas?

En relación a las repuestas anteriores, puede expresarse que existen dos frecuencias distintas. Solís y Alvarado manifiestan en una misma línea que el Internet ha permitido la facilidad para trascender fronteras convirtiéndose en una herramienta relevante para el desarrollo del comercio, la industria y la educación, no sólo en Guatemala sino en todo el mundo, y que esto, al mismo tiempo que esto ha creado una nueva forma para realizar actividades atípicas.

Por otra parte, el experto número 3 hace mención sobre la inversión significativa que aún debe realizarse en el territorio nacional sobre el uso de internet que va de la mano de una orientación hacia el buen manejo de los medios electrónicos que permiten su acceso. Esto significa que el desconocimiento sobre las implicaciones

que conllevan el uso de los mismos puede generar un riesgo para el desarrollo de actividades ilegales aprovechando la vulnerabilidad de los nuevos usuarios.

Pregunta #3 ¿Qué incidencia ha tenido la normativa internacional en la regulación de la actividad desarrollada en Internet?

En análisis a las respuestas brindadas por los expertos, se debe recalcar la incidencia importante con la que cuenta la normativa internacional en el ámbito informático. Las relaciones inter personales entre usuarios en internet generan actividades transfronterizas en las cuales puede en algún caso vulnerarse la integridad de la persona. En ese sentido la normativa internacional, como lo puntualiza De León con el Convenio de Budapest, contempla una regulación adecuada estableciendo una política para la seguridad cibernética. El Convenio al cual se hace mención, que también fue descrito en el capítulo 3 de esta investigación, significó un magno avance para el desarrollo de estrategias para la sanción y prevención de delitos cibernéticos. Guatemala daría un paso importante en este ámbito si se adhiere al presente Convenio puesto que está abierto para todos los países que quieren formar parte del mismo.

Pregunta #4: En Guatemala, ¿De qué manera ha existido algún tipo limitación que ocasione la falta de regulación a estas actividades de manera concreta?

Al responder esta interrogante, Solís y Alvarado expresan, en una misma línea que existen regulaciones de protección que se encuentran dispersas y no adecuadamente puntualizadas para actividades informáticas. Existe una carencia de un cuerpo normativo en materia de delitos informáticos y esto conlleva a que en el territorio guatemalteco exista una vulnerabilidad para el desarrollo de las éstos. Por otra parte, De León expresa que en Guatemala, la OEA conjunto con el Ministerio de Gobernación está desarrollando un plan denominado Estrategia de Seguridad Cibernética que, citando su respuesta, comenta que busca la integración de todas las entidades de gobierno relacionadas de manera directa e indirecta la

Seguridad Nacional, incentivando la participación de otros sectores como el privado, financiero y académico.

En concreto y aplicando lo detallado en la presente investigación, se puede manifestar que en Guatemala la regulación en materia informática es escasa si se compara a otros países de tal manera que para la integración de modalidades de protección deben las entidades pertinentes encargarse de promover la participación en búsqueda de una estrategia efectiva para la regulación de las actividades ilícitas en internet. En esa misma línea, De León expresa además que, a la fecha de la entrevista siendo el 30 de octubre de 2017, se han presentado dos iniciativas de ley en materia de ciberdelitos al Congreso de la República de Guatemala, siendo la iniciativa número 4055 y la número 5254, mismas que en el capítulo 3 de la presente investigación fueron expuestas.

Conforme lo anterior, la falta de regulación adecuada significa un riesgo evidente para la protección de derechos de las personas, ya que en cierta forma se evidencia la falta de interés y continuidad por parte de las autoridades para llevar a cabo un plan de acción en esta materia.

Pregunta #5 ¿Cuál es su opinión acerca de la plataforma conocida como Deep Web o Internet Profunda?

En respuesta a la presente pregunta, existen dos frecuencias diferentes. La primera correspondiente a describir la plataforma de la Deep Web como un sitio peligroso que mayormente promueve las actividades criminales y prohibidas por la ley penal. La segunda, según lo expresan Alvarado y De León, se desarrolla en relacionar esta plataforma como un sitio que contiene información reservada o acceso restringido al cual no se tiene acceso por medio de los motores de búsqueda convencionales. Este contenido almacenado corresponde a información académica, empresarial, financiera que por sus características y confidencialidad no pueden ser compartidas.

Sin embargo, De León puntualiza el término de *Dark Web,* mismo que es expuesto en el capítulo 1 de la presente investigación, el cual lo denomina como un sitio que cuenta con las características necesarias para realizar exclusivamente actividades ilícitas ya que se cuenta con la facultad de tener anonimato para la operación de las mismas. En concreto, en análisis de estas respuestas, se puede expresar que la Deep Web, como dato general, es aquel sitio en la Internet cuyo contenido no se encuentra indexado y por consiguiente no puede accederse a través de los motores de búsqueda convencionales lo cual viene a denominarse como confidencialidad de información según sus fines. Sin embargo, ante esta facultad de confidencialidad se han abierto las brechas para que se desarrollen actividades de carácter ilícito, espacio que se le denomina *Darknet* o *Dark Web.*

Pregunta #6 ¿Por qué este sitio es un espacio que se limita a la facilidad de realizar actividades ilícitas?

La frecuencia de la respuesta a la presente pregunta se genera de la siguiente forma: Solís expresa que es por la manera en que convergen criminales que usan la web para buscar nueva forma de delinquir. Por otra parte, Alvarado comenta que el factor clave es el ocultamiento. Y, por último, De León expresa, en ese sentido, que la *Dark Web* es el espacio ideal para la comisión de delitos, relacionando además el uso de las criptomonedas, o también conocidas como *bitcoins,* que facilitan el anonimato en transacciones de origen ilícito.

Al tomar en cuenta lo descrito en el párrafo anterior, puede recalcarse que, en virtud de la operación para la comisión de actividades ilícitas por parte de los criminales, es la *Deep Web* el espacio alternativo idóneo para llevar a cabo los delitos por el tipo de características que facilitan el desarrollo de las mismas.

Pregunta #7: ¿Qué posibilidad existe de que este campo pueda ser regulado con legislación concreta internacional?

Solís, al responder la interrogante, comenta, que las actividades que pueden desarrollarse en la Deep Web generalmente ya están tipificadas como delitos en legislaciones nacionales e internacionales, pero que debe ampliarse su aplicación. Alvarado manifiesta que toda información que sea lesionada debe regularse y sancionarse ya que sea en la internet profunda o la internet superficial. Tomando en cuenta esto, se puede interpretar que existe un criterio común en cuanto determinar como factor determinante la necesidad de regulación para las actividades ilícitas en Internet, que si bien es cierto existe cierta regulación en términos generales, ésta no es suficiente o no ha sido muy bien aplicada para el desarrollo de estrategias y planificación para el combate contra los delitos informáticos y cualquier actividad que lesione la información y sus atributos.

Por otra parte, De León expresa, que en la actualidad sólo son las potencias mundiales quienes cuenta con alguna regulación, que puede ser efectiva, y que en auxilio a su aplicación son las instituciones como la CIA, FBI, NSA, Interpol, entre otras, quienes se encargan de velar para el cumplimiento de estas normativas en materia. Además, comenta que, en el caso de Guatemala, es la PCN, MP e INACIF quienes cuentan con unidades de delitos cibernéticos donde atienden casos relacionadas a las actividades ilícitas que se desarrollan a través de la Internet, principalmente en tema de pornografía infantil, lo cual es un tema sensible y en crecimiento en la región.

Esto evidencia que aunque no se cuenta con una legislación expresa que sancione directamente estos delitos en Guatemala, si existen instituciones que velan por la protección de los derechos y bien común en internet y que por las limitaciones en cuanto a tecnificación y especialización para la erradicación de las mismas, son estas instituciones quienes deben, en el desarrollo de la persecución de las figuras delictivas, contar con los conocimientos y mecanismos necesarios y actualizados

para llevar a cabo su función como entes de cooperación en contra de las actividades ilícitas informáticas.

Pregunta #8 ¿Cómo puede llegar a afectar a Guatemala la existencia de este espacio en la red?

Guatemala como cualquier país puede ser afectado por la existencia de este espacio en la red por la realización de actos que afectan la información; así lo comentan en síntesis Solís y Alvarado. Sin embargo, De León en distinta línea comenta que no necesariamente la existencia de este espacio incide directamente para la realización de ilícitos, puesto que en la actualidad los criminales hacen uso de cualquier medio que la internet ponga a su disposición para cometer actividades que no van acorde a la moral, principalmente donde los jóvenes por su vulnerabilidad al cambio y adaptación a las nuevas tecnologías son los más impactados.

En un ambiente fuera de la Deep Web en donde se tiene a la internet superficial pueden encuadrarse muchas actividades ilícitas con herramientas de fácil acceso, como por ejemplo las redes sociales y las facilidades para distribución de material pornográfico. El internet que no conoce límites se ha convertido en un espacio para el almacenamiento de información de todo tipo y es evidente que de alguna manera ésta en algún momento desde su creación procediera a convertirse en un lugar para la comisión de delitos debido al uso inapropiado que usuarios con un fin malicioso desarrollan mecanismos para lograr su cometido. De cualquier forma, cualquier país en el planeta queda vulnerado sin los medios de protección de información adecuados.

Pregunta #9 ¿Cómo considera que el acceso anónimo hacia contenido clasificado ha afectado la integridad y privacidad de los usuarios virtuales en Internet?

Para responder esta interrogante se evidencian tres frecuencias distintas, una de ellas por Solís puntualizando que el anonimato facilita la suplantación de identidad que también es conocido como *Phising.* Alvarado comenta que los actos a razón del anonimato lesionan la privacidad agregando que los parámetros de lesión deben medirse tomando en consideración el patrimonio o integridad de la persona. Estos factores expuestos por los entrevistados van de la mano con lo relacionado a las facilidades que brinda el anonimato para la facilidad de comisión de delitos en donde la privacidad y acceso a la información quedan vulnerados.

De León, por su parte, expresa que, en el sentido de privacidad en contraste con la seguridad, los ciudadanos deben exigir a las empresas tecnológicas y gobiernos los medios para proteger su privacidad e integridad. De igual forma, agrega que es evidente que los usuarios en muchas circunstancias son poco precavidos con la información que comparten en la red ya que esta misma puede ser utilizada por cualquier persona malintencionada.

Relacionado al párrafo anterior, se puede comentar que en principio el usuario es completamente responsable por la información que comparte en la red y que por algún tipo de descuido u omisión a alguna norma de privacidad puede llegar a afectarse a sí mismo por el hecho que esta información pueda llegar a ser utilizada con fines maliciosos. Las entidades encargadas por velar por la seguridad de los usuarios no serían, en ese sentido, las únicas de poder contrarrestar actividades ilícitas informáticas, sino también los usuarios pueden contribuir a un buen manejo de información cuando se toman las precauciones debidas para impedir que la información contenida en la web sea utilizada de mala manera.

No en todas las ocasiones que un usuario tenga la oportunidad de acceder al internet tendrá los conocimientos necesarios para saber los buenos usos que deben dársele a ésta ya que hoy en día esta plataforma está al alcance de todas las personas y esto ha conllevado que en gran medida se incrementen las violaciones

hacia los derechos de terceros cuando el internet es utilizado de una manera incorrecta y que atenta contra bien común y a la buena fe.

6.1.2 Segundo Modelo de Entrevista

Pregunta #1 ¿Cómo ha sido su experiencia al ingresar a la Internet Profunda?

La frecuencia de respuesta que se obtiene a la presente pregunta obedece a que, en cuestión de experiencia, ésta se ha obtenido por razones al trabajo que desempeñan los entrevistados. De esta forma, se recalca que esta experiencia ha dejado entrever que no hay que tomar a la ligera el ingresar a la Deep Web ya que deben contarse con las medidas de seguridad necesarias para no ser rastreado por otros usuarios. Barrera compara lo anterior, como caminar por calles oscuras de un barrio peligroso ya que existen todo tipo de amenazas.

La Deep Web, como se desarrolla en el capítulo 1 de esta investigación y como lo ha sido expuesto por los entrevistados, es un sitio peligroso en el sentido que la navegación en ella conlleva ciertos riesgos a los cuales el usuario queda vulnerable sino cuenta con los medios de protección adecuados. La falta de atención y cuidado ante estas amenazas pueden significar un daño inminente hacia el usuario y los dispositivos que éste utiliza para navegar en la red.

Pregunta #2 ¿Qué riesgos o amenazas considera que pueden surgir en el acceso a la misma?

En relación a esta pregunta, Navas comenta que al conectarse a la red de TOR (*The Onion Router)*, descrita en el capítulo 1, puede convertirse en un medio de transmisión de contenido desconocido, lo cual incrementa el riesgo de ser afectado por usuarios maliciosos. Por otra parte, Morales expresa que para ingresar a cierto sitio debe antes conocerse, o sea ser consciente de que se quiere visitar, ya que existen maneras de rastrear la identidad y ubicación de quienes ingresan a ciertas

páginas, por lo que no es recomendable acceder a éstos sin tener la protección adecuada para impedir ser atacado programas malignos. Por último, Barrera expresa que la falta de experiencia puede conllevar a caer en trampas que esta red origina y que por consiguiente son perjudiciales para el usuario.

De esta forma, se puede agregar en sentido de análisis a lo anterior, que es evidente que sea cual sea el motivo por el cual alguna persona ingrese a este sitio debe tomar las precauciones debidas, ya que el descuido o mal conocimiento sobre navegación puede conllevar a ser afectado por peligros inminentes.

Pregunta #3 ¿Qué habilidades y destrezas son necesarias para ingresar a la internet profunda?

La frecuencia de respuestas para esta pregunta va en una misma línea según lo expuesto por los entrevistados, debido a que se concuerda que para ingresar y navegar en la Deep Web no se necesita de alguna habilidad o destreza especial. Sin embargo, Navas agrega que, aunque no se necesita cierta habilidad si debería tenerse un conocimiento sobre trasfondo de las consecuencias que conllevan visitar este sitio.

Pregunta #4 ¿Cuál fue el motivo que lo movió a ingresar a la Internet Profunda?

Los entrevistados para responder la presente pregunta concuerdan que es a razón de su profesión y por lo que su trabajo les demanda que deben conocer el tipo de riesgos y amenazas cibernéticas que surgen en la actualidad a través de Internet.

Pregunta #5 ¿Cataloga al uso de este espacio como un sitio meramente peligroso para la comunidad virtual?

En una misma frecuencia de respuesta los expertos comentan como dato común que es necesaria la experiencia y conocimiento para poder navegar de forma

adecuada, no solamente en la Deep Web, sino el en la internet en general y por consiguiente, se corren riesgos si no se cuenta con las medidas adecuadas.

6.2 Discusión y Análisis de Resultados

Al concretar la información brindada por los expertos y confrontarlo con el marco teórico de la presente investigación dan como resultado ciertos puntos de análisis que se señalan a continuación.

Se debe partir sobre lo relacionado acerca de las nuevas brechas que internet ha abierto en la sociedad de hoy en día a tal punto que ahora se cataloga como un recurso necesario para la comunicación y obtención de información; además, puede afirmarse que ésta ha obtenido un papel determinante en el presente siglo que se ha caracterizado por la evolución de las nuevas tecnologías. El acceso a la red se ha concretizado a tal punto de que cualquier persona que no tenga la oportunidad de acceder a la misma se encuentra alejada de la sociedad actual.

Por otro lado, el contar con un ordenador o cualquier tipo de dispositivo que brinde acceso a internet no hace al usuario totalmente conocedor de las implicaciones y responsabilidades que puede llegar a conllevar. Para todo aquel que cuente con las herramientas necesarias para navegar por la red debe poseer los conocimientos adecuados que le ayuden a garantizar seguridad ante cualquier riesgo o amenaza que pueda presentarse a través de la navegación en la red.

Sin embargo, aunque el Internet que está cada vez al alcance de todas las personas, el término Deep Web o Internet Profunda es hasta tal punto desconocido para muchos usuarios comunes que prefieren limitarse a la parte más superficial de internet antes que arriesgarse a entrar esta plataforma a razón de escepticismo o de ignorancia a la misma. Los expertos, en ese sentido de acuerdo con el primer modelo de entrevista, han dejado en evidencia que por el tipo de contenido que esta puede contener puede ser peligroso y que en virtud del resguardo de la integridad

de los usuarios no es recomendable ingresar sino se cuentan con las precauciones necesarias.

Además, debe afirmarse que no es solamente esta plataforma la que permite la comisión de delitos a grandes rasgos, sino que en la misma internet superficial se llevan a cabo actividades delictivas que ponen en peligro la integridad de los usuarios, ya sea personal, patrimonial, financiera, etc. A partir de ello, surge la necesidad de una protección y sanción penal para sufragar el desarrollo de cualquier hecho ilícito, y por tal motivo los organismos internacionales y nacionales deben elaborar una serie de mecanismos que garanticen las condiciones óptimas para que la sociedad de hoy en día y futuras generaciones puedan tener acceso a la red garantizando su protección.

No debe dejarse a un lado, que por la evolución y cambios que son evidentes en las tecnologías de la actualidad debe existir un constante mejoramiento y actualización de mecanismos para el combate de cualquier actividad anómala desarrollada en internet. Esto quiere decir, que todo aquello que ponga en peligro la creación y difusión de contenidos debe ser erradicado.

Hay cuerpos normativos que han significado los primeros pasos hacia la regulación en materia informática, sin embargo, esta ha quedado insuficiente como es el caso de Guatemala en donde hasta el día de hoy no existe una ley específica en materia de delitos informáticos y las iniciativas de ley en esta materia que han sido presentadas al pleno del Congreso de la República de Guatemala no han sido promulgadas.

Al hablar de la Deep Web no puede dejarse a un lado el relacionarla con lo denominado con los delitos informáticos o ciberdelitos, además de la temática de acceso a la información y privacidad de usuarios por el motivo que entre estos términos siempre existirá un denominador común que se explica a través del desarrollo de la comunicación que Internet permite. Al ser un espacio abierto a la

libertad de operación de usuarios es vulnerable hacia la comisión de actividades catalogadas como ilícitas que atentan contra los derechos de las personas, en el sentido que estas pueden llegar a impactar en el mundo real.

La Deep Web, entre todas sus características que le dan su razón de ser, ha logrado posicionarse como una herramienta para facilitar cualquier acto delictivo, tomando en cuenta en otra tangente que contiene información que por su naturaleza es confidencial, como se ha expresado por parte de los expertos. La falta de intangibilidad donde se desarrollan actividades informáticas anómalas junto con el factor de anonimato ha logrado obstaculizar las normativas legales y persecución penal. De acuerdo con ello si se desarrolla algún intento de culminar con el anonimato y socavar la identidad del criminal significa evidentemente un desafío de replantear los límites entre lo público y lo privado para cualquier usuario.

Es por ello, que el Derecho se ve obligado a manifestarse sobre la vulneración de los derechos fundamentales del ser humano, y, en el caso del Internet, y como los expertos hacen hincapié, es la ausencia de límites geográficos para fijar fronteras que determinen la protección de los usuarios.

Por otro lado, la normativa propia del derecho interno de cada país es fundamental y necesaria para garantizar la protección de los derechos de la persona y en esa misma línea al tratarse de una plataforma que tiene un uso constante debe reforzarse de la forma más atenta y posible adaptando preceptos reguladores de convenios y legislación internacional en materia.

En virtud de lo anterior, también se debe puntualizar que en cierto modo no es conveniente dejar la seguridad informática en manos de autoridades estatales y normativas específicas por el motivo que esta carga recae también en los propios usuarios puesto que por el simple de hecho de ser creadores y receptores de contenido informático deben generar actitudes enfocadas a la conciencia colectiva sobre la responsabilidad de cualquier actividad en donde se ven involucrados

derechos, libertades y bienes patrimoniales que pueden ser amenazados por su utilización indebida en internet.

CONCLUSIONES

1. La Deep Web o Internet Profunda 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.

2. La libertad que proporciona la internet, por su propia naturaleza, permite la facilidad de la comisión 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.

3. En el marco referido, 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.

4. Es indispensable el fortalecimiento y mejoramiento de instituciones que velen por la protección de los derechos fundamentales de los usuarios de internet además de actualizar constantemente las medidas de seguridad para impedir la comisión de delitos informáticos que puedan ocasionarse ya sea en la Internet Profunda o internet superficial.

RECOMENDACIONES

1. Se sugiere al Estado de Guatemala fortalecer su normativa en materia informática como prioridad, así como de delitos informáticos en particular, a efecto de crear un marco jurídico que esté concorde a los convenios internacionales sobre ciberdelincuencia que son de naturaleza transnacional.

2. Se exhorta a las instituciones encargadas de la persecución penal en Guatemala que fortalezcan sus mecanismos para implementación de planes y estrategias para combatir la ciberdelincuencia.

3. Se invita a los usuarios guatemaltecos a generar actitudes enfocadas a la conciencia colectiva sobre la responsabilidad que significa cualesquiera actividades desarrolladas en la red ya sea superficial o profunda.

4. Desarrollar procedimientos especiales que conlleven la promoción, la protección y el disfrute de los derechos humanos, así como el uso de Internet y tecnologías, considerando que éste no debe ser un medio de propagación del crimen, si no como una importante vía de comunicación en la sociedad actual.

REFERENCIAS

Referencias Bibliográficas:

1. Altmark, Daniel Ricardo y Eduardo Molina Quiroga. *Informática y Derecho. Aportes de Doctrina Internacional*. Volumen VI. Argentina. Ediciones Depalma. 1998

2. Arroyo Zapatero, Luis y Adán Nieto Martín. *Código de Derecho Penal europeo e internacional.* España. Ministerio de Justicia de España. 2008.

3. Ambos, Kai. *El derecho penal frente a amenazas extremas.* España. Editorial Dykinson. 2007.

4. Becerra Ramírez, Manuel y Rocío Ovilla Bueno. *El desarrollo tecnológico y la propiedad intelectual.* México. Instituto de Investigaciones Jurídicas – UNAM. 2002.

5. Brocos Fernández, José y Carolina Salinas Pardo. *Selección de recursos de información disponibles en el web invisible.* Argentina. Editorial Scielo. 2007.

6. Bustos Ramírez, Juan. *Manual de Derecho Penal.* España. Editorial Ariel. 1991. 2da. Edición.

7. Castillo, José Luis. *Virus Informático.* México. El Cid Editor. 2009

8. De León Velasco, Héctor Aníbal y José Francisco de Mata Vela. *Derecho Penal Guatemalteco: Parte General y Parte Especial.* Guatemala. Editorial Magna Terra. 2012. 22va. Edición.

9. Flores Salgado, Lucerito. *Derecho Informático.* México. Laurousse – Grupo Editorial Patria. 2014.

10. García Barrera, Myrna. *Derecho de las Nuevas Tecnologías.* México. Instituto de Investigaciones Jurídicas – UNAM. 2005.

11. García de la Cruz, Juan Manuel. *Delitos Informáticos.* México. El Cid Editor. 2009.

12. González, Jorge A. y otros. *Cibercultura e iniciación en la investigación.* México. Colección Intersecciones. 2007.

13. Jiménez de Asúa, Luis. *Lecciones de Derecho Penal.* México. Editorial Mexicana. 1997. 2da. Edición.

14. Lima Malvido, María de la Luz *Delitos Electrónicos.* Academia Mexicana de Ciencias Penales. México. Editorial Porrúa. 2004

15. Llobet Colom, Juan Antonio. *El Derecho de Autor, la legislación de Centroamérica y Panamá*. Guatemala. Editorial Piedra Santa.

16. Martínez Solórzano, Edna Rossana. *Apuntes de Derecho Informático.* Guatemala. Ediciones Mayte. 2012.

17. Miguel Asensio, Pedro Alberto. *Derecho Privado de Internet.* España. Editorial Civitas. 2015. 3ra. Edición.

18. Morales, Ronald y Rolando Alvarado. *Cibercrimen*. Guatemala. IUS Ediciones. 2012.

19. Nava Garcés, Alberto Enrique. *Análisis de los Delitos Informáticos.* México. Editorial Porrúa. 2005.

20. Nova Labián, Alberto José. *La propiedad intelectual en el mundo digital.* España. Ediciones Experiencia. 2010.

21. Ordoñez Solís, David. *La protección judicial de los derechos en Internet en la jurisprudencia europea.* España. Editorial Reus. 2014.

22. Quian, Alberto. *El impacto mediático y político de Wikileaks: la historia más apasionante del periodismo moderno*. España. Editorial UOC. 2013.

23. Rico Carrillo, Mariliana. *Derecho de las nuevas tecnologías.* Argentina. Ediciones La Rocca. 2007.

24. Rodríguez Cano, Rodrigo Bercovitz et. al. Manual de Propiedad Intelectual. España. Editorial Tirant Lo Blanch. 2004. 4ta. Edición.

25. Téllez Valdés, Julio. *Derecho Informático.* México. Editorial McGraw-Hill 1996. 2da. Edición.

Referencias Normativas:

1. Asamblea Nacional Constituyente. *Constitución Política de la República de Guatemala* 1985 y sus reformas.
2. Congreso de la República de Guatemala. *Código Penal.* Decreto Número 17-73. 1973 y sus reformas.
3. Congreso de la República de Guatemala. *Ley de Derechos de Autor y Derechos Conexos.* Decreto Número 33-98. 1998 y sus reformas.
4. Congreso de la República de Guatemala. *Ley de Propiedad Industrial.* Decreto Número 57-2000. 2000 y sus reformas.
5. Congreso de la República de Guatemala. *Iniciativa de Ley No. 4055: Ley de Delitos Informáticos.* 2009

6. Congreso de la República de Guatemala *Iniciativa de Ley 5254: Ley contra la ciberdelincuencia.* 2017.

Referencias Electrónicas:

1. ABC Tecnología. Espinosa, José Luis. *Los Peligros de Deep Web, la internet profunda.* España. 2015. Disponible en: http://www.abc.es/tecnologia/redes/20150708/abci-deepweb-secretos-internet-oculta-201507072005.html

2. ADSL ZONE. González, Carlos. *La Deep Web no es un lugar para impulsivos, morbosos e inexpertos.* España. 2015. Disponible en: https://www.adslzone.net/2015/06/14/la-deep-web-no-es-lugar-para-impulsivos-morbosos-e-inexpertos/

3. ADSL ZONE. González, Carlos. *Por qué Tor funciona lento, y como se puede navegar más rápido por la Deep Web.* España. 2015. Disponible en: https://www.adslzone.net/2015/09/23/por-que-tor-funciona-lento-y-como-se-puede-navegar-mas-rapido-por-la-deep-web/

4. Almudi. Piciarelli, Fabrizio. *El «Deep Web»: el lado oscuro de Internet. Un viaje más allá de las fronteras de la red.* España. 2017. Disponible en: https://www.almudi.org/noticias-articulos-y-opinion/11416-el-deep-web-el-lado-oscuro-de-internet-un-viaje-mas-alla-de-las-fronteras-de-la-red

5. Biblioteca Pleyades. Chandler, Nathan. *Cómo funciona la Internet Profunda.* Estados Unidos. 2015. Disponible en: http://www.bibliotecapleyades.net/sociopolitica/sociopol_internet214.htm

6. BITCOIN. *¿Qué es Bitcoin? Preguntas Frecuentes.* Estados Unidos. 2016. Disponible en: https://bitcoin.org/es/faq#que-es-bitcoin

7. BITCOIN. *Silk Road como herramienta para reducir la violencia.* Estados Unidos. 2016. Disponible en: http://elbitcoin.org/silk-road-como-herramienta-para-reducir-la-violencia-en-los-mercados-de-drogas/

8. Centro contra la Censura y Centro de Estudios Legales Aplicados. Universidad de Witwatersrand, en Johannesburgo. *Los Principios de Johannesburgo sobre Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información.* Reino Unido. 1996. Disponible en: https://www.article19.org/data/files/medialibrary/1803/Johannesburg-Principles.Spa.pdf

9. Colombia Digital. Àlvarez, Eliana. *Internet Profunda: concepto, características y niveles.* Colombia. 2014. Disponible en: https://colombiadigital.net/actualidad/noticias/item/6558-internet-profunda-concepto-caracteristicas-y-niveles.html

10. Cornell University Library. Nicholas Christin. *Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace.* Estados Unidos. 2012. Disponible en: https://arxiv.org/abs/1207.7139

11. Corporación Universitaria Americana. Majarrés, Iván y Farid Jiménez. *Caracterización de los delitos informáticos en Colombia.* Colombia. 2012. Disponible en: http://www.coruniamericana.edu.co/publicaciones/ojs/index.php/pensamientoamericano/article/viewFile/126/149

12. Electronic Frontier Foundation. *Anonimato y Cifrado.* Estados Unidos. 2015. Disponible en: https://www.eff.org/files/2015/03/18/anonimatoycifrado-eff-11.pdf

13. Estados Miembros de la Unión Europea. *Dcsición Marco 2005/222/JAI.* Bélgica. 2005. Considerando II. Disponible en: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2005:069:0067:0071:ES:PDF

14. Expansión. Pagliery, José. *Deep Web, el Internet que desconoces.* México. 2014. Disponible en: http://expansion.mx/tecnologia/2014/03/10/las-profundidades-del-mar-de-internet

15. Gobierno de España. Ministerio de Asuntos Exteriores y Cooperación. *Historia y Actividad del Consejo de Europa.* España. 2016. Disponible en: http://www.exteriores.gob.es/Portal/es/PoliticaExteriorCooperacion/ConsejoDeEuropa/Paginas/HistoriaActividadConsejoEuropa.aspx

16. Hempyreum. "*Deep Web" narra la historia del mártir de la guerra contra las drogas.* Suiza. 2015. Disponible en: http://www.hempyreum.org/arc/es/71782

17. La Penúltima. *Silk Road: El tráfico de drogas abre su tienda en internet.* España. 2012. Disponible en: http://lapenultima.org/silk-road

18. Magazine Digital. García, Juan Manuel. *Cien horas en la Internet Profunda*. España. 2016. Disponible en: http://www.magazinedigital.net/historias/reportajes/cien-horas-en-internet-profunda

19. Noriega Salazar, Hans Aarón. *Delitos Informáticos.* Instituto de la Defensa Pública Penal. Guatemala 2011. Disponible en: http://descargas.idpp.gob.gt/Data_descargas/Modulos/delitosinformaticos.pdf

20. Observatorio Para la Cibersociedad. Salazar García, Idoia. *La Red Profunda. Lo que los buscadores convencionales no encuentran.* España. 2004. Disponible en: http://www.cibersociedad.net/congreso/comms/g20salazar.htm

21. Oficina de las Naciones Unidas contra la Droga y el Delito. UNODC. *Tráfico de Drogas en Centroamérica y el Caribe.* Austria. 2014. Disponible en: https://www.unodc.org/ropan/es/BorderControl/drug-trafficking.html

22. Organización de las Naciones Unidas, Oficina Contra la Droga y el Delito. Boletín Informativo Undécimo Congreso Sobre la Prevención del Delito y la Justicia Penal 18 al 25 de Abril 2005 Bangkok Tailandia. Austria. 2005. Disponible en: http://www.unis.unvienna.org/pdf/05-82113_S_6_pr_SFS.pdf

23. Organización Mundial de la Propiedad Intelectual (OMPI). *Tratado de la OMPI sobre el derecho de autor.* Suiza. 2016. Disponible en: http://www.wipo.int/treaties/es/ip/wct/

24. Proyecto Idis. *Activismo Hacker*. Canadà. 2013. Disponible en: http://proyectoidis.org/activismo-hacker/

25. Rebelión. Martínez, David. *The Deep Web; los suburbios de Internet*. Estados Unidos. 2013. Disponible en: http://www.rebelion.org/docs/162798.pdf

26. Semantic Scholar. Bergman, Michael K. *The Deep Web: Surfacing Hidden Value.* Estados Unidos. 2000. Disponible en: https://www.semanticscholar.org/paper/The-Deep-Web-Surfacing-Hidden-Value-BERGMAN/0a59b63213f26b4e695ee01065163ba1769cf861

27. Temperini, Marcelo Gabriel Ignacio. *Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1era. Parte.* Argentina. 2013. Página 5 Disponible en: http://conaiisi.unsl.edu.ar/2013/82-553-1-DR.pdf

28. TrendMicro. Ciancaglini, Vincenzo y otros. *Below de Surface: Exploring the Deep Web.* Alemania. 2015. Disponible en: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp_below_the_surface.pdf

29. United Nations. *UN human rights chief voices concern at reported "cyber war" against WikiLeaks.* Estados Unidos. 2010. Disponible en: http://www.un.org/apps/news/story.asp?NewsID=37009#.Whas9xOCzq0

30. Universidad CEU San Pablo. Miguel Ramos López-Quesada. *Deep Web.* España. 2015. Disponible en: http://informaticaemprendimiento.org/wp-content/uploads/2015/05/ramos-DEEP-WEB-1.pdf

31. Universidad Técnica Federico Santa María. Departamento de Informática. *Legislación acerca del uso de Internet.* Chile. 2014. Página 1. Disponible en: www.inf.utfsm.cl/~lhevia/asignaturas/infoysoc/topicos/Etica/8_legislacion_acerca_uso_internet.pdf

32. Universitat Oberta de Catalunya. Tabóas, David. *¿Qué esconde la Deep Web?* España. 2016. Disponible en: https://www.uoc.edu/portal/es/uoc-news/actualitat/2016/043-deep-web.html

33. Wikileaks. *What is Wikileaks.* Holanda. 2016. Disponible en: https://wikileaks.org/What-is-Wikileaks.html

Referencias Normas Internacionales:

1. Asamblea General de las Naciones Unidas. *Declaración de los Derechos del Niño.* 1959. Principio IX.
2. Asamblea General de las Naciones Unidas. *Declaración de Viena sobre la delincuencia y la justicia: frente a los retos del siglo XXI.* Resolución 55/59. 17 de enero de 2001.

3. Estados Miembros del Consejo de Europa. *Convenio No. 108 del Consejo de Europa, de 28 de Enero de 1981, para la protección de las personas respecto al tratamiento automatizado de datos de carácter personal.* 1981.

4. Estados Miembros de la Unión Europea. *Desición Marco 2005/222/JAI.* Bélgica. 2005. Considerando II.

5. Jefatura de Estado de España. Ley orgánica 10/1995, de 23 de noviembre. Código Penal de España.

6. Organización Mundial de la Propiedad Intelectual (OMPI). *Tratado de la Organización Mundial de la Propiedad Intelectual sobre Derechos de Autor.* 20 de Diciembre de 1996.

ANEXOS

ANEXO 1:

Primer Modelo de Entrevista

Entrevistado:

Fecha de Entrevista:

1. ¿Qué importancia tiene la regulación de las actividades que se desarrollan en Internet?

2. ¿De qué manera considera que el internet ha significado una herramienta indiscutible para el desarrollo de muchos países, incluyendo a Guatemala, así como la facilidad para la elaboración de actividades ilícitas?

3. ¿Qué incidencia ha tenido la normativa internacional en la regulación de la actividad desarrollada en Internet?

4. En Guatemala, ¿ha existido algún tipo limitación que ocasione la falta de regulación a estas actividades de manera concreta y, si es así, de qué manera se ha dado?

5. ¿Cuál es su opinión acerca de la plataforma conocida como Deep Web o Internet Profunda?

6. ¿Por qué consideraría que este sitio es un espacio que se limita a la facilidad de realizar actividades ilícitas?

7. ¿Qué posibilidad existe de que este campo pueda ser regulado con legislación concreta internacional?

8. ¿Cómo puede llegar a afectar a Guatemala la existencia de este espacio en la red?

9. ¿Cómo considera que el acceso anónimo hacia contenido clasificado ha afectado la integridad y privacidad de los usuarios virtuales en Internet?

ANEXO 2:

Segundo Modelo de Entrevista

Entrevistado:

Fecha de Entrevista:

1. ¿Cómo ha sido su experiencia al ingresar a la Internet Profunda?

2. ¿Qué riesgos amenazas considera que pueden surgir en el acceso a la misma?

3. ¿Qué habilidades y destrezas son necesarias para ingresar a la internet profunda?

4. ¿Cuál fue el motivo que lo movió a ingresar a la Internet Profunda?

5. ¿Cataloga al uso de este espacio como un sitio meramente peligroso para la comunidad virtual?

ANEXO 3: ENTREVISTAS

Primer Modelo de Entrevista

Entrevistado: Lic. Carlos Alberto Solís Garza

Fecha de Entrevista: 06/09/2017

1. ¿Qué importancia tiene la regulación de las actividades que se desarrollan en Internet?

La importancia de regulación es vital para tener certeza jurídica de los derechos y obligaciones generadas por las relaciones contractuales de las partes mediante medios electrónicos. Asimismo, tipificar los delitos e infracciones que se pueden cometer en actividades que se desarrollan por internet.

2. ¿De qué manera considera que el internet ha significado una herramienta indiscutible para el desarrollo de muchos países, incluyendo a Guatemala, así como la facilidad para la elaboración de actividades ilícitas?

La llegada del Internet al mundo y a Guatemala vino a terminar con los espacios geográficos específicos y a trascender fronteras y ha sido una herramienta vital para el desarrollo del comercio en Guatemala y el mundo entero, facilitando la forma tradicional de hacer negocios. Y como contraparte se crea una forma nueva de hacer negocios en donde se pueden desarrollar fácilmente conductas atípicas e ilegales.

3. ¿Qué incidencia ha tenido la normativa internacional en la regulación de la actividad desarrollada en Internet?

La normativa internacional es relativamente nueva, pero en general se busca proteger a los ciudadanos de los países de actividades que se desarrollan en internet que atentan su integridad física, económica y moral. Muchos países han legislado internamente normas de protección para evitar abusos que pueden ser cometidos en internet.

4. En Guatemala, ¿ha existido algún tipo limitación que ocasione la falta de regulación a estas actividades de manera concreta y, si es así, de qué manera se ha dado?

Es cuestión que el Congreso de la República adopte regulaciones de protección, si bien encontramos algunas normas dispersas que regulan las actividades que se desarrollan en internet, no se cuenta con una regulación completa como en otros países.

5. ¿Cuál es su opinión acerca de la plataforma conocida como Deep Web o Internet Profunda?

Es peligrosa, ya que en ella se llevan a cabo mayormente actividades criminales y prohibidas por la ley penal mundial.

6. ¿Por qué consideraría que este sitio es un espacio que se limita a la facilidad de realizar actividades ilícitas?

Porque en él convergen criminales que utilizan el internet para buscar nuevas formas de delinquir, atraer a potenciales usuarios de sus productos ilícitos o explotar económicamente sus actividades ilícitas.

7. ¿Qué posibilidad existe de que este campo pueda ser regulado con legislación concreta internacional?

Las actividades ilícitas que se generan en la Deep Web normalmente ya son tipificadas como delitos en las legislaciones nacionales y los Convenios Internacionales, sería que se ampliara la acción de dichas normas a las actividades propias que se realizan en la Deep Web.

8. ¿Cómo puede llegar a afectar a Guatemala la existencia de este espacio en la red?

Como a cualquier país, la existencia de este espacio en la red, facilita la operación criminal dentro del país y por extranjeros. Por lo que desde ya dichas actividades la afectan.

9. ¿Cómo considera que el acceso anónimo hacia contenido clasificado ha afectado la integridad y privacidad de los usuarios virtuales en Internet?

La forma que afecta es a través de la suplantación de identidad y ser víctimas de Pishing.

Primer Modelo de Entrevista

Entrevistado: Lic. José Rolando Alvarado Lemus

Fecha de Entrevista: 25/08/2017

1. ¿Qué importancia tiene la regulación de las actividades que se desarrollan en Internet?
   Considero que la regulación de actos o hechos a través de Internet debe efectuarse únicamente en materia de Comercio Electrónico y Cibercrimen, para validar los actos y sancionar conductas ilícitas que perjudiquen a las personas.

2. ¿De qué manera considera que el internet ha significado una herramienta indiscutible para el desarrollo de muchos países, incluyendo a Guatemala, así como la facilidad para la elaboración de actividades ilícitas?
   Internet ha contribuido y contribuye en muchos factores, como el caso de la educación donde ha tenido un papel trascendental para que el conocimiento sea de acceso libre y en una forma automatizada; en el comercio, al facilitar la industria y comercio, haciéndolo agilizando los procedimientos de oferta, compra, venta y comercialización en general; comunicación: al generar la nueva tendencia de medios digitales, etcétera.

3. ¿Qué incidencia ha tenido la normativa internacional en la regulación de la actividad desarrollada en Internet?
   Debido a que son hechos transnacionales o transfronterizos, las leyes uniformes internacionales cumplen un papel muy importante, en cuanto a prevención y sanción de delitos y en cuanto a comercio electrónico.

4. En Guatemala, ¿ha existido algún tipo limitación que ocasione la falta de regulación a estas actividades de manera concreta y, si es así, de qué manera se ha dado?
   Sí, Guatemala tiene regulación de comercio electrónico pero carece de un cuerpo normativo en materia de delitos informáticos, lo cual nos convierte en un paraíso de actividades ilícitas a través de las nuevas tecnologías de la información.

5. ¿Cuál es su opinión acerca de la plataforma conocida como Deep Web o Internet Profunda?
   Existe información reservada o de acceso restringido que no debe publicitarse o accederse por medio de motores de búsqueda. Tenemos información confidencial, como secretos empresariales, patentes, asuntos de intimidad, etcétera que no debe

facilitarse su acceso. Además, la denominada Internet Profunda tiene un peso o tamaño mayor que, al tenerse acceso, complicaría la agilización de acceso a la información. Considero que es un tema relacionado con la confidencialidad de la información, ya que las personas no han querido indexarla por diversos motivos.

6. ¿Por qué consideraría que este sitio es un espacio que se limita a la facilidad de realizar actividades ilícitas?
   Pienso que por su ocultamiento. En materia de Cibercrimen la regla prevaleciente es el ocultamiento.

7. ¿Qué posibilidad existe de que este campo pueda ser regulado con legislación concreta internacional?
   Todo acto que lesione la información y sus atributos de confidencialidad, integridad y disponibilidad, debe regularse y sancionarse. Toda información contenida en un sistema informático debe protegerse, independientemente a que se encuentre en internet superficial o en la oculta.

8. ¿Cómo puede llegar a afectar a Guatemala la existencia de este espacio en la red?
   Por actos que afecten la información.

9. ¿Cómo considera que el acceso anónimo hacia contenido clasificado ha afectado la integridad y privacidad de los usuarios virtuales en Internet?
   Son actos que lesionan la privacidad y todo acceso indebido o sin autorización debe ser restringido y sancionado. Los efectos deben estimarse según casos concretos donde deben tenerse en cuenta parámetros de lesión, ya sea de índole patrimonial o en la persona. Como el caso del daño a personas y al patrimonio.

Primer Modelo de Entrevista

Entrevistado: Amilcar de León

Fecha de Entrevista: 30/10/2017

1. ¿Qué importancia tiene la regulación de las actividades que se desarrollan en Internet?

El mundo del ciberespacio no tiene límites, y su regulación, principalmente legal puede ser complicada. Sin embargo, es importante que esto se dé. Lo que vemos actualmente en Latinoamérica y el caribe, es que la mayoría de países no cuenta con una regulación adecuada como lo hacen países como Alemania, Inglaterra y Estados Unidos, por nombrar algunos. El inconveniente con no contar con regulaciones surge en varios niveles, desde normativas para el (mal) uso de herramientas en la nube por parte de menores de edad, como de cibercriminales para realizar actividades ilícitas.

2. ¿De qué manera considera que el internet ha significado una herramienta indiscutible para el desarrollo de muchos países, incluyendo a Guatemala, así como la facilidad para la elaboración de actividades ilícitas?

Guatemala cuenta actualmente con un 23% de penetración de internet a nivel de país (según la SIT). Esto refleja que todavía se requiere invertir enormemente en el acceso a internet, principalmente en el área rural. Sin embargo, este dato podría ser discutible si llegásemos a identificar la conexión de cada persona de manera única, al internet. Dicho esto, imaginemos que la población en el área rural, niños y jóvenes, tienen acceso a internet mediante dispositivos adquiridos de manera no oficiales (ej: compra venta ilegal o simplemente envío de regalos de familiares del extranjero), o café internet, y a esto le sumamos que éstos usuarios no cuentan con una adecuada orientación en el uso de las herramientas, se vuelven automáticamente potenciales víctimas de sexting, grooming e inclusive hasta trata de personas.

Por otro lado, desde el aspecto de desarrollo como país, definitivamente esto abre la puerta a innumerables posibilidades principalmente de desarrollo de negocios. Sin embargo, también es de resaltar que en Guatemala, el costo de adquisición de servicios de internet, tanto a nivel de casa como corporativo todavía es muy caro, si lo comparamos con las posibilidades de acceso que tienen países como Estados Unidos o España, donde puedes contratar un servicio residencial de 50mpbs por 20 Euros al mes.

3. ¿Qué incidencia ha tenido la normativa internacional en la regulación de la actividad desarrollada en Internet?

Existe una preocupación enorme en la región, por varias instituciones como la OEA, BID, y los gobiernos, de poder establecer Estrategias y Políticas de seguridad cibernética, que pudiese contemplar la adecuada regulación de las actividades en el ciberespacio. En Europa, se creó desde el 2001 el denominado "Convenio de Budapest", el cuál marca una pauta para que todos los países miembros colaboren entre sí para crear regulaciones que permitan la identificación, mitigación y concientización de temas como delito cibernético. Hoy en día, el convenio está a abierto a adherir a otros países, incluso fuera de Europa; México y Chile por ejemplo ya han sido adheridos.

4. En Guatemala, ¿ha existido algún tipo limitación que ocasione la falta de regulación a estas actividades de manera concreta y, si es así, de qué manera se ha dado?

En Guatemala, la OEA en conjunto con el Ministerio de Gobernación está liderando el desarrollo de una Estrategia de Seguridad Cibernética, que busca por supuesto la integración de todas las entidades de gobierno relacionadas de manera directa e indirecta con la Seguridad Nacional, como el Ministerio de la Defensa, Policía Nacional Civil, Ministerio Público, SAAS, CONRED, entre otras; pero también está incentivando la participación de otros sectores como el privado, financiero y académico. La iniciativa está muy buena, pero puede verse que algunos sectores no están muy bien representados, por falta de interés. Es importante que todas estas instituciones (principalmente fuera de gobierno) participen de manera proactiva para logra que esta estrategia sea una realidad. Por otro lado, también se tienen al día de hoy, dos iniciativas de ciberdelito, la 4055 (presentada en 2011) y la 5254 (presentada en 2016). Actualmente el proceso para dar lectura en el congreso y realizar las respectivas aprobaciones, de cualquiera de las dos, está demorando bastante. Puedo pensar que es por algunas otras prioridades que tienen las autoridades para revisar este tipo de iniciativas.

5. ¿Cuál es su opinión acerca de la plataforma conocida como Deep Web o Internet Profunda?

Deep web es toda aquella información que no está almacenada en los índices de los motores de búsqueda, como información académica, de empresas, que, cuyas plataformas de almacenamiento han sido deliberadamente configuradas para no compartir estos datos. Por otro lado, existe el término Dark Web, la cuál es conocida por realizar actividades ilícitas como compra/venta de drogas, armas hasta trata de personas. La dark web no puede ser accedida por navegadores web convencionales, sino con herramientas destinadas para este acceso como Tor, que mantienen el anonimato de los usuarios y los sitios hosteados en dicha red.

6. ¿Por qué consideraría que este sitio es un espacio que se limita a la facilidad de realizar actividades ilícitas?

En el caso de la dark web, pienso que es útil para realizar actividades ilíticas poruque mantiene el anonimato de los usuarios, es sumamente complicado identificar el origen de ciertas comunicaciones. Si mexclamos esto, con otras tecnologías como criptomonedas, es prácticamente imposible (hasta la fecha) lograr determinar qué usuario realiza qué transacciones, por qué motivo y en qué sitio. Es una alternativa genial para los cibercriminales.

7. ¿Qué posibilidad existe de que este campo pueda ser regulado con legislación concreta internacional?

Es complicado. Actualmente, solo las potencias mundiales tienen alguna regulación, además de la cooperación entre instituciones internacionales como CIA, FBI, NSA, Interpol, y algunas otras locales de cada país. Sin embargo, es de mencionar que muchos países se encuentran sumamente preocupados por el incremento de crímenes cibernéticos. En Guatemala, por ejemplo, PCN, MP e INACIF ya cuentan con unidades de delitos cibernéticos, donde si bien no pueden atender casos como hackeo de wifi, ataques de DoS, etc, están trabajando principalmente con el tema de Pornografía Infantil, que es un tema muy sensible y que se encuentra en crecimiento en la región. Aunque no se cuenta con regulación ni leyes (solamente iniciativas), las autoridades trabajan con lo poco que pueden y poco a poco se van tecnificando y especializando en éste tipo de actividades, como los peritajes forenses digitales.

8. ¿Cómo puede llegar a afectar a Guatemala la existencia de este espacio en la red?

Creo que no hace falta que este espacio exista o sea utilizado para actividades ilícitas. En la actualidad, los cibercriminales hacen uso del internet tradicional y herramientas en la nube de acceso a todo público como las redes sociales para llevar a cabo sus actividades ilícitas. Me refiero a por ejemplo sexting, grooming, distribución de drogas auditivas, cyberbullying, pornovenganza, y de hecho la juventud está experimentando excesivamente con los juegos sexuales y distribución de material pornográfico por las distintas redes sociales. Parte fundamental de ésta problemática se debe a la falta de orientación y educación desde los padres hasta los educadores en los establecimientos educativos. Todo esto sucede fuera del ambiente de la Deep o Dark web. Sucede con Facebook, Instagram, snapchat, etcétera. Herramientas de fácil acceso.

9. ¿Cómo considera que el acceso anónimo hacia contenido clasificado ha afectado la integridad y privacidad de los usuarios virtuales en Internet?

Creo que el debate en éste sentido es la privacidad vs. La seguridad. Los ciudadanos exigen privacidad por parte de las grandes empresas tecnológicas y gobiernos, y estos por el contrario violan en excesivo la privacidad de los usuarios, para fines comerciales,

pero también temas de seguridad (a través de cibersepionaje por ejemplo). Por otro lado, podemos tener iniciativas que buscan la transparencia como Gobierno Abierto/Electrónico, cuya razón de ser es garantizar la transparencia, pero como todo en este mundo, puede ser utilizado para fines ilícitos. Las empresas y gobiernos que almacenan datos sensibles deben estar conscientes de los cuidados que esto conlleva en el mundo cibernético, pero también otra realidad es que los usuarios son muy poco precavidos para controlar sus perfiles de privacidad en redes sociales, o publicar información que puede ser utilizada por cualquier persona malintencionada para ocasionar fraudes, estafas, extorsiones, entre otras.

Segundo Modelo de Entrevista

Entrevistado: Ing. Melinton Navas

Fecha de Entrevista: 06/09/2017

1. ¿Cómo ha sido su experiencia al ingresar a la Internet Profunda?

El uso de la *Deep Web* dentro del campo de seguridad informática no es muy común. Sin embargo, dentro del campo de la investigación de nuevas amenazas y demás, es una fuente que proporciona información sobre lo que se está comercializando en este aspecto. Su navegación sí requiere cierto detalle, ya que los sitios no están identificados por nombres de diccionario como la web que conocemos, y cambian constantemente.

2. ¿Qué riesgos amenazas considera que pueden surgir en el acceso a la misma?

En términos breves, al conectarse a la red de TOR (*The Onion Ring*) nuestro equipo se convierte en parte de la malla que conforma esta red completa. Esto quiere decir que estamos transmitiendo contenido que no conocemos, lo que incrementa el riesgo de vernos afectados si no tomamos las medidas adecuadas.

3. ¿Qué habilidades y destrezas son necesarias para ingresar a la internet profunda?

El conocimiento técnico de lo que se está haciendo al navegar por estos sitios es importante, más no necesario. En la actualidad es muy popular el compartir conocimiento por internet, por lo que basta con realizar una búsqueda rápida en Google, descargar lo necesario, y navegar por la *Deep Web* libremente, sin embargo, el conocer el trasfondo de lo que sucede al visitar todos estos sitios permite al usuario estar anuente de las implicaciones.

4. ¿Cuál fue el motivo que lo movió a ingresar a la Internet Profunda?

En mi caso, es investigativo, ya que cuando surgen nuevas amenazas cibernéticas, el primer lugar que habla de ellas son estos sitios y estos foros.

5. ¿Cataloga al uso de este espacio como un sitio meramente peligroso para la comunidad virtual?

El internet es básicamente un espacio enorme sobre el cual se desborda la información, desinformación y conocimiento. Esto incluye la *Deep Web*, ya que en las manos correctas, hay mucha información valiosa. Sin embargo, es importante tener en cuenta que el conocimiento técnico mencionado anteriormente es importante para protegernos de cualquier amenaza que se encuentre en estos espacios. Fuera de eso, el conocimiento es poder.

Segundo Modelo de Entrevista

Entrevistado: Ing. Ronald Morales

Fecha de Entrevista: 26/09/2017

1. ¿Cómo ha sido su experiencia al ingresar a la Internet Profunda?

Este tipo de navegación siempre obedece a cuestiones de trabajo, por lo que se ha realizado guardando las medidas de seguridad necesarias, tratando de evitar dejar rastros o ser ubicados dentro de esta área.

2. ¿Qué riesgos amenazas considera que pueden surgir en el acceso a la misma?

Regularmente, estos sitios requieren de autenticación o conocer el sitio que se requiere visitar, también tienen muchas formas de conocer quien entra y que origen, no es conveniente descargar SW de estos sitios o comprar herramientas sin tener una protección adecuada sobre exploits o malware.

3. ¿Qué habilidades y destrezas son necesarias para ingresar a la internet profunda?

Realmente no requiere mayores destrezas, más que conocer la forma de ingresar en ella, si la persona sabe cómo ingresar sabe también como protegerse.

4. ¿Cuál fue el motivo que lo movió a ingresar a la Internet Profunda?

Como mencione al principio, por cuestiones de trabajo relacionado a investigación.

5. ¿Cataloga al uso de este espacio como un sitio meramente peligroso para la comunidad virtual?

Si no se tiene experiencia y no se toman las medidas necesarias si, pero de igual manera si se navega en la web normal de manera poco cuidadosa igual se corre riesgos.

Segundo Modelo de Entrevista

Entrevistado: Ing. Juan Pablo Barrera

Fecha de Entrevista: 23/10/2017

6. ¿Cómo ha sido su experiencia al ingresar a la Internet Profunda?
   La experiencia de ingresar a la internet profunda es como caminar por las calles oscuras de un barrio peligroso. Uno debe cuidarse y estar muy atento ante cualquier amenaza.

7. ¿Qué riesgos amenazas considera que pueden surgir en el acceso a la misma?
   Es una red que esta plagada de trampas para novatos, alguien sin experiencia puede caer fácilmente en ellas.

8. ¿Qué habilidades y destrezas son necesarias para ingresar a la internet profunda?
   No se requiere ninguna habilidad especial para ingresar, mas bien saber descargar e instalar un software y buscar en Google.

9. ¿Cuál fue el motivo que lo movió a ingresar a la Internet Profunda?
   Mi profesión demanda el conocimiento de este tipo de riesgos para poder apoyar a los clientes en prevenir fuga de información hacia este lugar.

10. ¿Cataloga al uso de este espacio como un sitio meramente peligroso para la comunidad virtual?
    Es peligroso para cualquier persona que ingresa allí de manera inocente y sin experiencia.