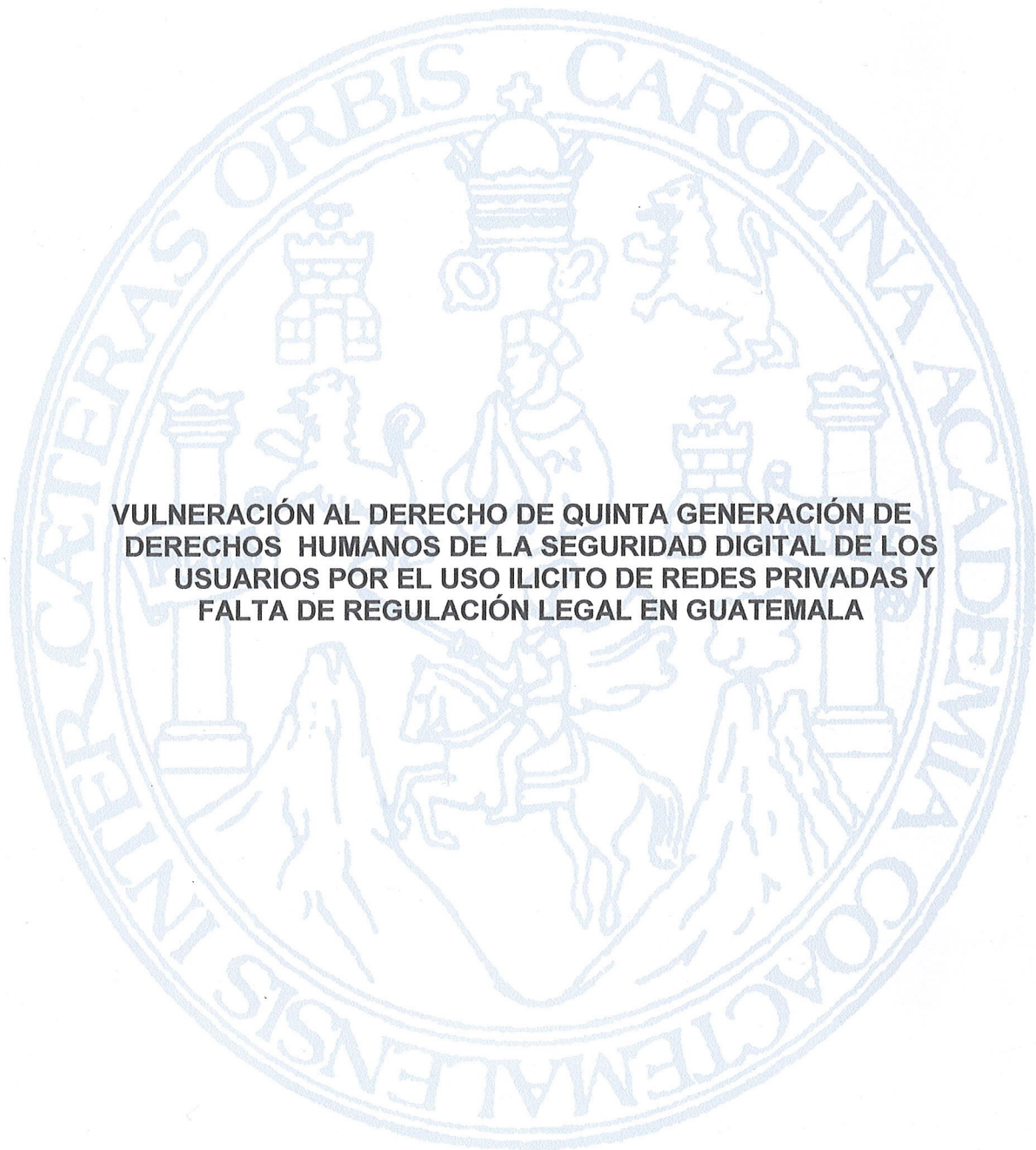


UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES



**VULNERACIÓN AL DERECHO DE QUINTA GENERACIÓN DE
DERECHOS HUMANOS DE LA SEGURIDAD DIGITAL DE LOS
USUARIOS POR EL USO ILÍCITO DE REDES PRIVADAS Y
FALTA DE REGULACIÓN LEGAL EN GUATEMALA**

KAREN VERÓNICA FORTÍN RAMÍREZ

GUATEMALA, NOVIEMBRE DE 2024

**UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES**

**VULNERACIÓN AL DERECHO DE QUINTA GENERACIÓN DE DERECHOS HUMANOS DE
LA SEGURIDAD DIGITAL DE LOS USUARIOS POR EL USO ILÍCITO DE REDES
PRIVADAS Y FALTA DE REGULACIÓN LEGAL EN GUATEMALA**

TESIS

Presentada a la Honorable Junta Directiva
de la

Facultad de Ciencias Jurídicas y Sociales
de la

Universidad de San Carlos de Guatemala

por **KAREN VERÓNICA FORTÍN RAMÍREZ**

Previo a conferírsele el grado académico de

LICENCIADA EN CIENCIAS JURÍDICAS Y SOCIALES

Y los títulos profesionales de

ABOGADA Y NOTARIA

Guatemala, NOVIEMBRE de 2024

**HONORABLE JUNTA DIRECTIVA
DE LA
FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES
DE LA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA**

DECANO: M. Sc. Henry Manuel Arriaga Contreras

VOCAL I: Vacante

VOCAL II: Lic. Rodolfo Barahona Jácome

VOCAL III: Lic. Helmer Rolando Reyes García

VOCAL IV: Lic. Javier Eduardo Sarmiento Cabrera

VOCAL V: Br. Gustavo Adolfo Oroxom Aguilar

SECRETARIO: Lic. Wilfredo Eliú Ramos Leonor

**TRIBUNAL QUE PRACTICÓ
EL EXAMEN TÉCNICO PROFESIONAL**

Primera Fase:

Presidente: Lcda. Blanca Maribel Alvarez Paredes

Vocal: Lic. Julio Roberto Pineda Garcia

Secretario: Lic. Jorge Eduardo Isaías Aguilar Soto

Segunda Fase:

Presidente: Lic. Eddy Azurdia

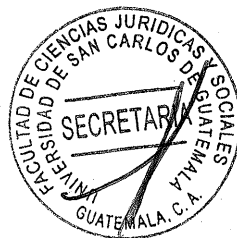
Vocal: Lcda. Marta Alicia Ramirez Cifuentes

Secretario: Lcda. Brenda Lisseth Ortiz Rodas

RAZÓN: "Únicamente el autor es responsable de las doctrinas sustentadas en la tesis". (Artículo 43 de Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público).



USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala



Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala,
29 de junio de 2023

Atentamente pase al (a) Profesional, **GUILLERMO DAVID VILLATORO ILLESCAS**, para que proceda a asesorar el trabajo de tesis del (a) estudiante **KAREN VERÓNICA FORTÍN RAMÍREZ**, con carné 201601327, intitulado: **VULNERACIÓN AL DERECHO DE QUINTA GENERACIÓN DE DERECHOS HUMANOS DE LA SEGURIDAD DIGITAL DE LOS USUARIOS POR EL USO ILÍCITO DE REDES PRIVADAS Y FALTA DE REGULACIÓN LEGAL EN GUATEMALA.**

Hago de su conocimiento que está facultado (a) para recomendar al (a) estudiante, la modificación del bosquejo preliminar de temas, las fuentes de consulta originalmente contempladas; así como, el título de tesis propuesto.

El dictamen correspondiente se debe emitir en un plazo no mayor de 90 días continuos a partir de concluida la investigación, en este debe hacer constar su opinión respecto del contenido científico y técnico de la tesis, la metodología y técnicas de investigación utilizadas, la redacción, los cuadros estadísticos si fueren necesarios, la contribución científica de la misma, la conclusión discursiva, y la bibliografía utilizada, si aprueba o desaprueba el trabajo de investigación. Expresamente declarará que no es pariente del (a) estudiante dentro de los grados de ley y otras consideraciones que estime pertinentes.

Adjunto encontrará el plan de tesis respectivo.



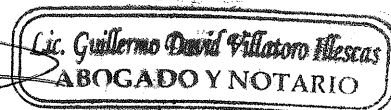
CARLOS EBERTITO HERRERA RECINOS

Jefe (a) de la Unidad de Asesoría de Tesis

SAQO

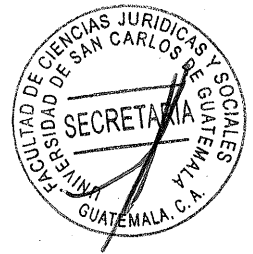
Fecha de recepción 14 / 09 / 2023. (f)

Asesor(a)
(Firma y sello)



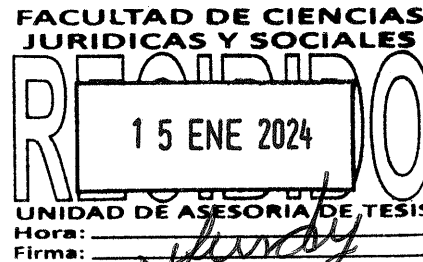


Villatoro e Illescas Asociados
Abogados y Notarios
Bufete Corporativo



Guatemala 20 de septiembre del año 2023.

Dr. Carlos Ebertito Herrera
Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala.
Su Despacho.



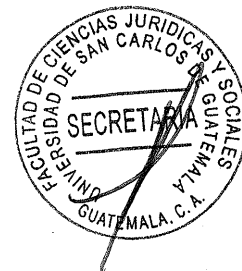
Me place saludarle deseándole los correspondientes éxitos en ese Despacho y demás labores profesionales.

En cumplimiento al nombramiento recaído en mi persona, en mi calidad de asesor del trabajo de tesis de la bachiller **KAREN VERÓNICA FORTÍN RAMÍREZ**, intitulado “**VULNERACIÓN AL DERECHO DE QUINTA GENERACIÓN DE DERECHOS HUMANOS DE LA SEGURIDAD DIGITAL DE LOS USUARIOS POR EL USO ILÍCITO DE REDES PRIVADAS Y FALTA DE REGULACIÓN LEGAL EN GUATEMALA**”. Es procedente dictaminar respecto a la asesoría del mismo debido a las siguientes justificaciones

- i. La estudiante **KAREN VERÓNICA FORTÍN RAMÍREZ**, en su trabajo de tesis, enfoca con bastante propiedad con apoyo en el derecho positivo y la doctrina, sobre la importancia de la protección de los derechos humanos y su vulneración al derecho de la quinta generación en la seguridad digital de los usuarios por el uso ilícito de redes privadas y su falta de regulación legal en Guatemala.
- ii. El tema es abordado en una forma sistemática, de fácil comprensión y didáctica, abarcando antecedentes, definiciones y doctrina, así como regulación legal en la materia, apoyando su exposición con fundamento en normas constitucionales y derecho ordinario aplicable al mismo, lo que hace de este trabajo un documento de consulta y utilidad a quien esa clase de información necesite.
- iii. Aunado a lo expuesto, se pudo establecer que el referido trabajo de investigación se efectuó apegado a la asesoría prestada, habiéndose apreciado el cumplimiento a los presupuestos tanto de forma como de fondo exigidos por el Artículo treinta y uno (31) del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público de la facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala, ya que las técnicas que se utilizaron fueron la documental y de fichas bibliográficas, con las cuales se recopiló la información actual y relacionada con el tema.
- iv. El contenido del trabajo de tesis tiene relación con la conclusión discursiva, siendo la bibliografía empleada la correcta y relacionada con las citas bibliográficas de los capítulos. A la sustentante, le sugerí ampliar sus capítulos, introducción y bibliografía, bajo el respeto de su posición ideológica; quien se encontró conforme



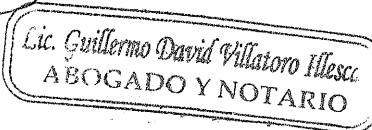
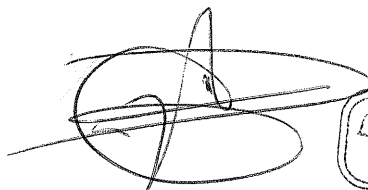
Villatoro e Illescas Asociados
Abogados y Notarios
Bufete Corporativo



con llevarlas a cabo, y por último pude constatar que la bibliografía era la adecuada para la elaboración del tema.

- v. El trabajo denota esfuerzo, dedicación y empeño y personalmente me encargué de guiarla durante las etapas del proceso de investigación científica, aplicando las técnicas de investigación y los métodos analíticos y sintéticos; con lo cual se comprobó la hipótesis planteada.
- vi. No fueron necesarios la presentación de cuadros estadísticos, debido a que la investigación no lo ameritaba.
- vii. El lenguaje empleado durante el desarrollo de la tesis es correcto y el contenido de la misma es de interés para la ciudadanía guatemalteca, siendo el trabajo un aporte técnico y científico para los estudiantes y catedráticos que manejen el tema de los derechos humanos especialmente en los derechos digitales.
- viii. Por lo expuesto concluyo que el trabajo de tesis, no se limita a cumplir únicamente con los presupuestos de presentación y desarrollo, sino también a la sustentación en teorías análisis y aportes tanto de orden legal como académica, ello en atención a los preceptos del normativo en mención regulados para el efecto, resultando como relevante el contenido analítico inserto en todo el trabajo de investigación.
- ix. Aunado a lo anterior manifiesto expresamente que con la bachiller, no me unen nexos de parentesco, amistad íntima o enemistad, ni cualquier otro tipo de relación que pudiera afectar la imparcialidad de este dictamen, la cual ofrezco sin ningún interés directo o indirecto.
- x. En consecuencia, en mi calidad de **asesor** de tesis me permito **DICTAMINAR FAVORABLEMENTE**, en el sentido de que el trabajo de tesis de grado de la autora amerita seguir su trámite hasta su total aprobación para ser discutido en su examen público de graduación y poder optar al grado académico de Licenciado en Ciencias Jurídicas y Sociales.

Sin otro particular me suscribo como su atento y seguro servidor.
Deferentemente;



Lic. Guillermo David Villatoro Illescas
Asesor.
Colegiado 12743



USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

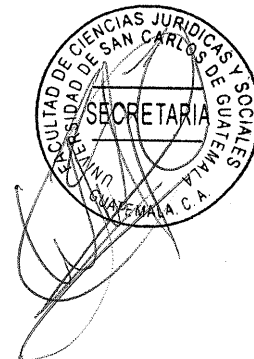
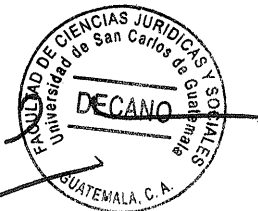
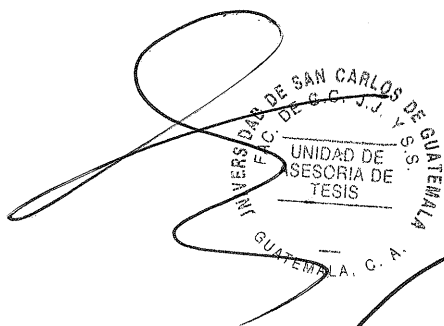


D.ORD. 715-2024

Decanatura de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala, nueve de julio de dos mil veinticuatro.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante, **KAREN VERÓNICA FORTÍN RAMÍREZ**, titulado **VULNERACIÓN AL DERECHO DE QUINTA GENERACIÓN DE DERECHOS HUMANOS DE LA SEGURIDAD DIGITAL DE LOS USUARIOS POR EL USO ILÍCITO DE REDES PRIVADAS Y FALTA DE REGULACIÓN LEGAL EN GUATEMALA**. Artículos 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

HMAC/JIMR





DEDICATORIA

- A DIOS:** Fuente de inspiración y bendición en mi vida.
- A MI PADRE:** Ronal Eduardo Fortín Morataya, gracias por su constancia, consejos, amor, sacrificio, guía, apoyo y ser un ejemplo a seguir. (Q.E.P.D.)
- A MI MADRE:** Thelma Verónica Ramírez por sus, consejos brindados, paciencia, ser ejemplo de amor, humildad, dedicación, constancia y paciencia.
- A MI HERMANA:** Thelma Lucrecia Fortín Ramírez gracias por la orientación, apoyo y ser un ejemplo a seguir.
- A MI ASESOR:** Licenciado Guillermo David Villatoro Illescas por la orientación, sus consejos y paciencia.
- A MI FAMILIA:** Por el apoyo que me han brindado.
- A MIS AMIGOS:** Por todos los momentos compartidos, su apoyo emocional y paciencia.



A:

La Tricentenaria Universidad de San Carlos de Guatemala, por los conocimientos compartidos, así como la transmisión de valores humanísticos que caracterizan a sus profesionales egresados de la misma.

A:

A la Facultad de Ciencias Jurídicas y Sociales, gracias por la apertura de sus puertas académicas que hoy permiten la culminación de una meta.

PRESENTACIÓN

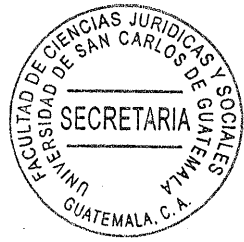


El presente trabajo de investigación, hace referencia que los sujetos de estudio son los usuarios que utilizan las redes privadas virtuales o por sus siglas en el idioma inglés VPN (Virtual Private Network), el objeto de estudio es la problemática en el uso ilícito, como medio para la comisión de hechos o actos delictivos, que vulneran el derecho a la seguridad digital de la población guatemalteca, perteneciente al conjunto de derechos humanos de quinta generación que surgen derivados del avance tecnológico mundial.

La temática abarca el ámbito constitucional, administrativo y penal, derivado que el Estado rige sus funciones y obligaciones jerárquicamente en la Constitución Política de la República de Guatemala, como norma suprema de la organización estatal, materializándose en una directriz para la realización o abstención de una acción humana, cuya contradicción conlleva a la imposición de una sanción administrativa o penal.

La presente investigación, tiene como finalidad dar a conocer la existencia de las VPN, la relevancia de su uso correcto, así como la forma para la autorización o prohibición contradictoria a su naturaleza, como una obligación a la protección de los derechos inherentes a las personas por parte del Estado de Guatemala; la misma es de índole cualitativa toda vez que se evaluó la seguridad, comprendido del periodo de 2019 al 2022. No se utilizaron cuadros estadísticos. Así mismo, la presente representa un aporte académico, técnico científico para los estudiantes y catedráticos que manejan el tema en relación con la seguridad digital.

HIPÓTESIS



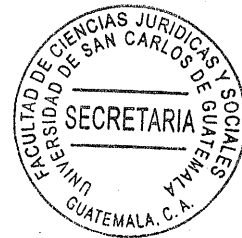
La falta de información, prevención y regulación específica del uso de redes privadas virtuales en Guatemala; vulnera el derecho humano de quinta generación, de la seguridad digital de los usuarios, por no garantizar la implementación controlada y efectiva, para el uso permisivo o prohibitivo de las mismas, lo cual desencadena en la materialización de figuras delictivas, tales como, la violación al derecho de autor, la propiedad industrial y delitos informáticos.

COMPROBACION DE LA HIPÓTESIS



El Estado de Guatemala, debe informar a las personas que lo habitan o residen, la existencia de las redes privadas virtuales, el uso correcto de las mismas o, en su defecto, regular su autorización o prohibición, para así cumplir con lo preceptuado en la Constitución Política de la República de Guatemala, en el sentido, que es deber del Estado garantizarle a los habitantes de la República, el bien jurídico tutelado de la seguridad, inclusive, la seguridad digital, como un derecho humano de quinta generación, el cual aplicado en materia constitucional, informático, penal y administrativo, es vulnerado por parte de las personas que utilizan los avances tecnológicos con fines ilícitos; en especial el uso ilícito de las funciones de las VPN.

A través del método analítico y deductivo empleado, se comprueba la hipótesis; ya que el primero, sirvió para análisis de la legislación, tipificando conductas ilícitas de las personas, contiene normas jurídicas, que abarcan los avances tecnológicos en las plataformas gubernamentales; el segundo, evidencia la falta de conocimiento, regularización jurídica y específica, de las VPN, como prevención a la materialización de conductas ilícitas.



ÍNDICE

Pág.

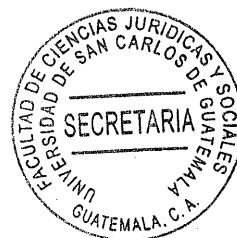
Introducción.....	I
-------------------	---

CAPÍTULO I

1. Nociones y terminología digital o tecnológica.....	1
1.1 Red privada y funciones.....	1
1.2 Peligro de Infecciones.....	8
1.2.1 Malware.....	11
1.2.2 Virus Troyanos.....	13
1.2.3 Spyware.....	15

CAPÍTULO II

2. El derecho de seguridad y seguridad digital.....	17
2.1 La seguridad y sus divisiones más comunes.....	18
2.2 Antecedentes del derecho a la seguridad digital.....	20
2.3 Alcances del derecho a la seguridad digital.....	24
2.4 Breve análisis de la normativa jurídica en Guatemala relacionada a la Seguridad digital de las plataformas de:.....	27
2.4.1 Registros de la propiedad.....	27
2.4.2 Registro mercantil.....	29
2.4.3 Superintendencia de Administración Tributaria.....	30



CAPÍTULO III

3. Derecho humano de la seguridad digital de quinta generación y el derecho comparado.....	33
3.1 Breve Análisis de los derechos humanos de quinta generación.....	35
3.2 Derechos humanos de seguridad digital y la normativa jurídica en México.....	36
3.3 Derechos humano de seguridad digital y la normativa jurídica en China.....	39
3.4 Derechos humano de seguridad digital y la normativa jurídica en Rusia.....	42

CAPÍTULO IV

4. Protección a la seguridad digital y las redes privadas virtuales.....	45
4.1 Plataformas virtuales como medio masivo informativo.....	48
4.2 Formas de regularización jurídica para uso, control y regulación de las redes privadas virtuales en Guatemala.....	50
4.2.1 Circulares Administrativas.....	54
4.2.2 Reglamentos.....	56
4.2.3 Normas Jurídicas Específicas.....	57
CONCLUSION DISCURSIVA.....	63
BIBLIOGRAFIA.....	65



INTRODUCCIÓN

Derivado, al creciente aumento a la vulneración al derecho digital, como derecho humano de quinta generación, tiene su nacimiento en la constante evolución de la humanidad y sus avances tecnológicos, los cuales son utilizados de forma ilícita por un grupo de personas, como medios para la comisión de delitos, por lo cual, tras brindar información del uso correcto de las redes privadas para su uso y control, proporciona un avance para la protección del mencionado derecho de forma individual, y prepara al Estado de Guatemala, para oportunamente crear una normativa jurídica específica para las mismas, o en su defecto, el establecimiento de las redes privadas virtuales que representen mayor confiabilidad para su uso y prohibición de aquellas que no lo sean.

La hipótesis planteada comprueba que el Estado de Guatemala, debe proporcionar conocimiento de las funciones y objeto de las redes privadas virtuales, a los internautas que se encuentran en el territorio guatemalteco, así como regular el uso, control, autorización o prohibición de las mismas, para evitar la comisión de hechos u actos ilícitos, cumpliendo con lo preceptuado en el Artículo 2 de la Constitución de la República de Guatemala, en el sentido que el deber del Estado es garantizarle a los habitantes de la República, el bien jurídico tutelado de la seguridad, esta incluye la seguridad digital.

El objetivo general de esta investigación, fue determinar la forma de garantizar el derecho a la seguridad digital, como derecho humano de quinta generación, a través de la divulgación de información del uso correcto de las redes privadas virtuales,

previniendo así, la comisión de ilícitos. En los objetivos específicos se establecieron las redes que pueden autorizarse o prohibirse, así como el explicar las formas para regularización del uso y control de las VPN, de esta forma, proporcionar una efectiva protección a la seguridad digital de las personas en Guatemala.

La investigación se dividió en cuatro capítulos: el primero, destinado a conocer las nociones y terminología que envuelven el mundo digital o tecnológico, para comprender el desarrollo y la importancia que representa el tema abordado, dedicado para tal finalidad; el segundo, aborda el desarrollado del derecho a la seguridad y la seguridad digital, en cuanto a la diferencia entre ambas; el tercero, hace referencia al desarrollo del derecho humano de quinta generación, y el derecho comparado, el cual nos permitirá estudiar a la brevedad la legislación relacionada a la investigación, culminando la misma con el capítulo cuarto, denominado como protección a la seguridad digital y las redes privadas virtuales, capítulo de gran importancia ya que en este, se desarrolla en punto exacto de nuestra temática de una forma directa y concreta.

Los métodos empleados, dentro del presente análisis fueron: científico, analítico, sintético, comparativo, inductivo, deductivo, y las técnicas de la investigación, como lo es el uso de plataformas virtuales; se planteó la conclusión discursiva correspondiente, con la cual, se comprobó la hipótesis planteada. Este conglomerado informativo proporcionado, brindará conocimiento a los futuros lectores, estudiantes, ciudadanos, nacionales o extranjeros, a los cuales se les instruye al uso correcto, lícito y seguro de las Redes Privadas Virtuales, para la protección de sus datos y demás vínculos personales, familiares y laborales.

CAPITULO I

1. Nociones y terminología digital o tecnológica

Para el desarrollo y comprensión de la presente investigación, es necesario hacer de nuestro conocimiento algunos términos referentes a la tecnología, que nos ayuden a comprender el funcionamiento de las redes privadas virtuales tales como:

1.1. Red privada

“Es aquella red exclusiva de una sola compañía u organización en particular”.¹ Cuya función consiste en ser un tipo de red que brinda mayor seguridad, al ser utilizada de forma supervisada por un administrador o proveedor del servicio, el cual puede ser internet o una red de área local LAN.

Red de computadora: “La cual consiste en un grupo de computadoras conectadas entre sí que comparten información y recursos”.² Dicha conexión forma un cúmulo de información, que a través de cifrados logra establecer una conexión, o varias de estas a las que se les denomina red.

Red de Área local LAN: Es de importancia hacer mención de esta red, ya que a través de ella es que se establece la conexión y puente para el uso de las VPN, y consiste en:

¹González Morales, Alexandro. **Redes privadas virtuales**. Pág. 2.

² **Ibid.** Pág. 2.



una “red donde todas las computadoras conectadas en red están dentro de una habitación, un edificio e incluso varios edificios dentro una localidad pequeña”.³

Red pública: “Es una red a través de la cual circula información de muchas compañías y organizaciones”.⁴ Este tipo de red es la que más se utiliza en lugares concurridos como plazas, comerciales, parques recreativos, estacionamientos, restaurantes, etc.

Administrador de Red: Consiste en el distribuidor de conexión, es el encargado de otorgar permiso, negar el mismo o establecer conexión a través de este. En el recae la responsabilidad de control, supervisión, manejo y distribución de las conexiones en una lugar, empresa o web.

Web: Es un conjunto de información, de códigos y datos que se encuentran en una dirección determinada en el internet. Estas direcciones pueden ser una o varias.

Servidor: “Es aquella computadora que proporciona funciones o servicios a otras computadoras.”⁵ Entendido como un medio, una plataforma o conglomerado de datos que forman un acceso para la conexión de datos. Entre estos encontramos: servidores de archivo, internet, de red. Sirven como contenedores de información, datos y lenguaje de programación destinados a la consulta de los usuarios para obtener información o entretenimiento.

³ **Ibíd.** Pág. 3.

⁴ **Ibíd.** Pág. 7.

⁵ **Ibíd.** Pág. 10.

Datos: Consisten en la individualización de características que hacen único a un servidor, persona, sistema o componente electrónico. Son representaciones simbólicas, numéricas, alfanuméricas, que contienen un atributo o variable, que puede ser cuantitativo o cualitativo, describen y codifican un hecho, un suceso o una entidad.

Sistema: Es conocido como sistema web, y no es más que un conjunto de aplicaciones, que pueden ser usados a través de un servidor o mediante un navegador, para captar información, posteriormente almacenarla y procesarla para la realización de operaciones con ella.

Navegador: Es un software o un programa, que permite la interpretación de códigos HTML, se introduce en el conjunto de interfaz gráfica que conforma una web. Es el más utilizado por los usuarios, internautas y cibernautas, para realizar búsquedas informativas o para diversión de los usuarios, a través de juegos virtuales que no necesitan instalación alguna.

Internet: Si bien, la presente investigación no tiene como punto principal el conocer que es el internet, este es de gran importancia, ya que a través de la misma se desarrollan los escenarios tanto para prevención, uso y control de las redes privadas virtuales. Sin este elemento, no existiría una investigación y muchos otros elementos que dan motivo a la misma. El internet es una red de computadoras que interconectadas a nivel mundial en forma de tela de araña, transmiten información entre sí, conformada por un aproximado de cien mil millones de personas conectadas entre ellas a través de redes telefónicas o cable.

Dirección IP: Es una dirección única que identifica a un dispositivo en internet o una red local, la cual la hace única entre el resto. Son un identificador que permite el envío de información entre dispositivos en una red. Equivale a la denominación que posee cada ser humano para ser distinguido dentro de la sociedad a la que pertenece, o individualiza.

Cada IP o protocolo de internet, "se encuentra formado por una cadena de números que pueden variar de 0 a 225, y son asignadas por la Autoridad de números asignados de internet llamada *Internet Assigned Numbers Authority IANA*, a través de una división de internet denominada *Internet Corporation* para números y nombres asignados".⁶

Modo incógnito: Es una ventana privada de un navegador web, por medio del cual se brinda una protección del registro, ya que a través de esta pestaña, no se guardan los datos de registro en un historial de un dispositivo. A diferencia de una VPN el modo incógnito no puede utilizar un servidor proveniente del extranjero, conserva su IP el dispositivo y no la oculta, facilitando a las instituciones encargadas de una investigación la detección del origen del dispositivo que la utilizo.

Cifrado: Consiste en un codificar datos para que puedan ser leídos por los servidores, usuarios o sitios web autorizados y que posean los medios para devolverlos a su estado original. y así poder observar el contenido de su codificación. Traslada la información primaria en un lenguaje de programación para ser leído con programas claves.

⁶ KASPERSKY. **Qué es una dirección IP: definición y explicación.** <https://latam.kaspersky.com/resource-center/definitions/what-is-an-ip-address> (Consultado el 05 de diciembre 2022).



Software: Es término informático que se refiere a un programa de cómputo, que permite la realización de distintas tareas en un sistema informático. Dicho *software* puede ser el responsable de la ejecución de todas las aplicaciones que hacen funcional un sistema de cómputo para que opere correctamente. Así como utilizarle para el desarrollo de uno nuevo o en su defecto puede estar codificado en forma de aplicación para ser utilizado en la realización de tareas en un dispositivo.

Encontramos distintas funciones de un *software*, pero este puede ser utilizado de forma maliciosa o malintencionado, denominado como *malware*, este es creado con fines ilícitos para obtener información o datos privados de un usuario de la web o internet, puede ser causal de daño de sistema, así como robo de identidad y mal funcionamiento de las funciones básicas y de seguridad de un dispositivo.

Hardware: Podemos afirmar que el *hardware* es el complemento del *software*, consistente en la parte física de un ordenador o sistema informático, conformado por componentes que pueden ser electrónicos, mecánicos y/o electromecánicos, cables, placas, discos duros, mouse, teclado, etc.

Es importante para la ejecución de las tareas de un dispositivo, ya que sin la parte material de este no pueden ejecutarse los comandos propios para el manejo de la tecnología.

Red Privada Virtual: El término más importante en el desarrollo de nuestra investigación. Una vez comprendido los distintos términos básicos que componen parte

de las conexiones que forman el conglomerado de aplicaciones, información y programas dentro del internet, podemos abordar el siguiente concepto.

Denominadas VPN, por sus siglas en inglés, que significan Virtual Private Network (Red Privada Virtual). Son un modo de establecer una conexión segura protegida al utilizar redes públicas, las cuales cifran los datos en internet y disfrazan la identidad de un usuario en línea. Dichas VPN, si se destinan para la función que fueron creadas garantizan proveer seguridad a todas las personas que las utilicen, sin embargo, el disfraz que utilizan para la protección puede convertirse en una herramienta de doble filo, ya que al mismo tiempo que permite ocultar la identidad por seguridad, también permite ocultar la identidad para hacer difícil la localización de la IP del dispositivo que se está utilizando.

Las redes privadas virtuales, permiten utilizar un servidor de otro país, las cuales permiten ocultar datos de ubicación demográficos, que no guardan registro de la actividad del uso de las mismas. Es decir, una persona que se encuentra en Guatemala puede utilizar una VPN para ocultar su IP y de esta forma dejar un registro falaz que se encuentra o estuvo en una localización geográfica distinta, como lo es, y a manera de ejemplo, Países Bajos.⁷

Uso ilícito de la VPN: Dentro del uso ilícito para el que pueda destinarse una red privada virtual, encontramos: conectarse a la red pública utilizando una red privada para enviar

⁷ Digital guide ionos. **Direcciones IP: todo lo que debes saber.** <https://www.ionos.es/digitalguide/servidores/know-how/direccion-ip/> (Consultado el 5 de diciembre de 2022).

mensajes a otra persona con contenido engañoso, denigrante, amenazador, intimidador o enviar un link, que almacene datos personales, cuentas bancarias, correos, fotografías, ubicación; para lo cual observamos en la norma un efecto castigador de la acción ilícita cometida, mas, no tiene un efecto preventivo, informativo, permisivo o controlador, tal como lo evidencia el Decreto Número 17-73 Código Penal de Guatemala, De los Delitos Contra el Derecho de Autor, La Propiedad Industrial y Delitos Informáticos, en su Artículo 274 F, el cual establece " Se impondrá prisión de seis meses a dos años, y multa de doscientos a mil quetzales al que, sin autorización, utilizare los registros informáticos de otro, o ingresare, por cualquier medio, a su banco de datos o archivos electrónicos".

Otros ilícitos que emanan del uso incorrecto de sus funciones, utilizando el caso expuesto con anterioridad, encontramos: la simulación del lugar de ubicación de conexión, o paradero exacto de la personas que utiliza la VPN, estafa, discriminación, amenazas, violación a la intimidad sexual. Derivado de la obtención, sin consentimiento de fotografías; coacción, enriquecimiento ilícito, entre otros delitos de los contemplados en el código antes mencionado. (Decreto Número 17-73 Código Penal de Guatemala, 2022). Y las nuevas figuras como: ciberacoso, bullying electrónico, creación de perfiles falsos y páginas web diseñadas para el robo de datos personales o privados.

Aplicaciones: Son herramientas cuya función es la realización de operaciones o funciones específicas, diseñadas para facilitar el ejercicio o ejecución de una tarea haciéndola más sencilla. Generalmente ejecutan funciones repetitivas en forma de ciclo.

Existen aplicaciones nativas, así como aplicaciones web, diferenciándose una de la otra por la forma en la que se han programado.⁸

Programas: Los programas son secuencias, instrucciones que se ejecutan para la realización de funciones que pueden ir acompañadas de un medio, como lo son las aplicaciones. Es un conjunto de procesos orquestados que cumplen una función específica, controlan el funcionamiento de programas preinstalados en el computador.

Conexión: Es un vínculo, un medio por el cual se transfieren datos codificados y sin codificar, ya se forma alámbrica (con cableado) o de forma inalámbrica (sin cable). Puede ser considerada como una frecuencia que une a una o más computadoras entre sí.

1.2 Peligro de infecciones

El presente apartado, contiene el desarrollo de las formas en las que puede ocurrir una infección en el sistema, o en su defecto, las circunstancias que hacen vulnerable las aplicaciones, sistemas o plataformas electrónicos que utilizan las personas al momento de navegar en el internet o en la web, y su relación con las redes privadas virtuales. Evidenciando así la existencia de múltiples amenazas a los sistemas tecnológicos, del mismo modo que el poco desarrollo de defensas, que protejan el *software* y el *hardware* de las computadoras que contienen almacenadas la información de los usuarios.

⁸ GoDaddy. **Qué es una app, para qué se utiliza y qué tipos existen.** <https://es.godaddy.com/blog/ que-es-una-app-y-para-que-se-utiliza/> (Consultado el 5 de diciembre de 2022).

Hackers: Como principal circunstancia a desarrollar, que pone en peligro el derecho a la seguridad digital de los usuarios que residen en Guatemala y otras partes del mundo, encontramos el ataque realizado por los *hackers*.

Un *hacker*, es una persona que vulnera la seguridad de una computadora o sistema de comunicación para obtener información, o dañar dispositivos a través de pruebas de nuevas formas de infección virtual, como lo es un virus.

Se desconoce el móvil que influye en el actuar de dichos vulneradores, ya que puede ir desde un fin económico y social, hasta el mero hecho de diversión, es decir, estos personajes realizan este tipo de acciones ilícitas con la finalidad de divertirse o probar nuevas formas de infección que conllevan a la pérdida de información personal, bancaria o privada.

Existe una clasificación, según las finalidades que se han detectado en forma general, siendo los más importantes para la presente:

Sombrero blanco: son los que fabrican un software malicioso, con el objeto de desarrollar una protección contra los mismos, comúnmente los crean personas que trabajan en una empresa de seguridad cibernética,⁹ para desarrollar posibles defensas que prevengan el ataque de los mismos.

⁹ Wikipedia. **Hacker seguridad informática**. [https://es.wikipedia.org/wiki/Hacker_\(seguridad_informática\)](https://es.wikipedia.org/wiki/Hacker_(seguridad_informática)) (Consultado 5 de diciembre 2022).

Sombrero negro: Es el tipo de *hacker* al cual el público los considera como criminales informáticos, ya que estos entran en las redes para destruir los datos o inutilizar las mismas para evitar su acceso autorizado.

Sombrero gris: Son el tipo de hacker que media entre el blanco y negro, ya que estos tienen la finalidad de violentar la seguridad para que el administrador a cargo, descubra los puntos que pueden ser vulnerados, mismos que serán reparados por la persona que los violentó.¹⁰

Parches: Los parches en la informática, hacen referencia a los cambios que se realizan en un programa, con el objetivo de corregir errores, actualizar información, encriptar y sustituir información; son creados por personas ajenas a los autores o creadores de los programas originales, como ejemplo: encontramos los antivirus.

El peligro de infección, en este medio lo encontramos en los simuladores que se encuentran programados para ejecutarse una vez se ejecute el parche, es decir, en lugar de instalar una corrección del programa, se instalará un software malicioso que pondrá en riesgo la seguridad digital de la persona que lo ha instalado.

Infección por virus: Las infecciones por virus, son las que ocurren derivado de software maliciosos, que infectan los datos que se encuentran encriptados en un sistema, programa o archivo de datos.

¹⁰ Tecinnova. **Hacker de sombrero negro, blanco y gris**. <https://www.tec-innova.mx/hackers-de-sombrero-negro-blanco-y-gris/> (Consultado el 5 de diciembre de 2022).

Es la principal causa de vulneración digital que es conocida por los usuarios del internet o navegantes.

Encontramos entre los virus más comunes: los que se alojan en memorias USB, los de tipo de acción directa que afecta los ficheros y archivos al ejecutarse, los de sobreescritura que se encargan de borrar la información de dichos ficheros, los de sector de arranque, que afectan el inicio del disco duro, virus polimórfico que utilizan diferentes algoritmos.¹¹

Dentro de las circunstancias que vulneran la seguridad jurídica encontramos dos importantes software maliciosos, los cuales se detallan a continuación.

1.2.1 Malware

La presente amenaza tiene destinado un inciso para su abordaje, derivado que es el tipo de infección más conocida por los usuarios que utilizan la web y el internet.

Consiste en *software* malicioso que es dañino para los sistemas, ya que es de comportamiento hostil, intrusivo e intencionalmente desagradable; invade los sistemas, ordenadores y sistemas informáticos para dañarlos. Así mismo, suele tomar control de las funciones y operaciones de los dispositivos, provocando el mal funcionamiento de la

¹¹ KYOCERA. **8 tipos de virus informáticos que debes conocer.** <https://www.kyocera documentsolutions.es/es/smarter-workspaces/insights-hub/articles/8-tipos-virus-informaticos-debes-conocer.html> (Consultado el 5 de diciembre de 2022).

aplicación, tales como: lentitud del programa, fallas en la ejecución del mismo, pantallazos, entre otros.¹²

Entrando así propiamente a la materia que nos corresponde abordar, la intención del malware es la vulneración al derecho de seguridad digital, violentándolo con la finalidad de obtener datos privados para hacer uso de las cuentas bancarias, monetarias o de índole pecuniaria que tenga la persona que ha sido afectada con este *software* malicioso. Al utilizar una red privada virtual la persona o *hacker* que introdujo el *software* malicioso puede dificultar su localización geográfica, así como su IP.

Entre las posibles soluciones para evitar ser víctima de *malware*, encontramos, el evitar el uso de aplicaciones ajenas a los proveedores originales y no certificados, la no instalación de parches creados por autores anónimos, la protección en contraseñas con el uso de mayúsculas, símbolos y lenguaje alfanumérico. Así mismo, borrar el historial que contenga *cookies* y registros, una vez terminadas las transacciones bancarias, derivado que esta clase de virus puede realizar una búsqueda de los rastros de los registros que dejan nuestras acciones virtuales.

En conclusión, el malware, es un *software* malicioso, creado con la intención de obtener datos personales, privados y bancarios, para obtener un enriquecimiento ilícito, violentando la seguridad digital de los usuarios que utilizan la red, internet o web, tanto en la República de Guatemala como en el resto del mundo con acceso a la red mundial.

¹² MALWARE. **Todo acerca de malware.** <https://es.malwarebytes.com/malware/> (Consultado el 5 de diciembre de 2022).

1.2.2 Virus Troyanos

El derecho a la seguridad digital se encuentra en constante vulneración, derivado de la existencia de los *softwares* y *malwares* existentes y otros que se encuentran en desarrollo. Esta clase de *malware* es conocido como el caballo de Troya por el relato mitológico. Considerado como una de las amenazas más peligrosas y molestas que se ha desarrollado durante el avance tecnológico. En su momento fue reconocido como un truco brillante y una hazaña asombrosa, pero hoy es considerada como un peligro digital, cuyo único propósito es causar estragos en los ordenadores de los usuarios infectados, sin que lo sepan.

La principal forma de operar de este *malware* para violentar el derecho a la seguridad digital, consiste en la lectura de las contraseñas, ya que registra las pulsaciones en el teclado o abre puertas de acceso para la entrada de más malware, que podrían incluso tomar el control de las funciones del ordenador.

Ejecutan en segundo plano ataques como:

- Borrar y eliminar datos.
- Bloqueo de contraseñas, bases de datos y sistemas.
- Creación de copias o duplicados del contenido de los datos del usuario.
- Interrumpen el rendimiento y funcionamiento de los dispositivos electrónicos y computarizados.

Existen troyanos de puerta trasera, los cuales crean un enlace que puede cargar todo tipo de malware en el sistema u ordenador de la persona que ha sido infectada, convirtiéndose en el más peligroso de los *malware*.

Los *malware exploit* consisten en programas que contienen datos o códigos que se aprovechan de la vulnerabilidad dentro de una aplicación. Contrario a los *malware Dropper*/ troyanos de descarga; consisten en incorporar otros programas de *malware* consigo mismo, al momento de su ejecución, por ejemplo: el troyano bancario *Trickbot* y el *ransomware Ryuk*. Se diferencian de los antes mencionados, ya que para poder ejecutarse necesitan de otros programas o un recurso de red.

Los troyanos bancarios, son los que afectan las cuentas bancarias de los usuarios, es decir, violentan los sistemas de seguridad bancario en relación a la seguridad digital, por medio de técnicas como el *phishing*, el cual consiste en enviar a las personas una página manipulada para que estas introduzcan sus datos y credenciales de acceso y obtenerlas así de forma ilícita. Pese a los esfuerzos y constante actualización que el sistema bancario realiza para prevenir y erradicar este tipo de vulneración, la tecnología continúa avanzando y representa un reto para concretar tal finalidad.¹³ Hoy en día observamos un crecimiento de acciones ilícitas que se relacionan o derivan de la expansión y compartimiento de este virus, ya sea implantado de forma directa, utilizando un disfraz electrónico con una denominación distinta, o adherida a algún programa, aplicación, sistema, emulador o juego, que se ejecuta al iniciar el *software*.

¹³ ACADEMY. **Qué es un malware troyano guía definitiva.** <https://www.avast.com/es-es/c-trojan> (Consultado el 06 de diciembre de 2022)

1.2.3 Spyware

Es el tipo de *malware* que intenta mantenerse oculto, haciendo un registro de información en secreto y realiza un seguimiento de las actividades en línea o rastro virtual, tanto en equipos de cómputo, como en dispositivos electrónicos. La principal función de esta amenaza es el rastreo, la supervisión y duplicado que escribe, carga y descarga, y almacena en segundo plano, los datos.

Es preocupante la existencia de esta amenaza, ya que sirve como medio para el robo de datos, contraseñas y demás, la cual sirve para suplantar la identidad, siendo esta una situación grave, puesto que se da un robo de identidad, con lo que pueden efectuar movimientos ajenos al titular de los datos y realizar transferencias de los mismos.

Existen tipos de *spyware*, siendo el primero el *keylogger*, que consiste en el registro de las pulsaciones de teclas presionadas por el usuario, en los dispositivos electrónicos para su autoguardado y así extraer la información de forma ilícita.

El *adware* como un variante del *spyware*, funciona a través de anuncios que el administrador coloca en las páginas web, de los cuales, el creador de la amenaza infecta, para que a través de estos despliegue ventanas emergentes que contienen enlaces, imágenes, videos o páginas en blanco, cuya finalidad es la implantación de la amenaza para que inicie con el duplicado ilícito de información.



Sin importar la denominación que se emplee para referirnos a las amenazas que actualmente se han desarrollado, como resultado del uso y avance tecnológico, no deja de ser preocupante el crecimiento de usuarios que destinan las VPN para usos ilícitos, cambiando el principal objetivo de creación de las mismas.

Guatemala, como garante de la seguridad del usuario debe implementar un método efectivo que cumpla con proporcionarles seguridad digital efectiva, lo cual representa un verdadero reto, tanto para el mencionado Estado, como para el resto del mundo, ya que los sistemas electrónicos-cibernéticos presentan un rápido y constante avance, dificultando su normativa, su restricción o autorización.

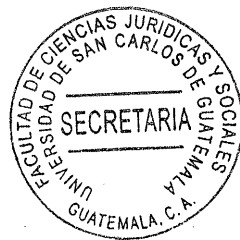
CAPITULO II

2. El derecho de seguridad y seguridad digital

El derecho a la seguridad, consiste en la protección inherente que posee toda persona para sentirse libre, protegido y seguro durante el desarrollo de sus actividades cotidianas, personales, sociales, políticas y económicas. Siendo una obligación del Estado de Guatemala velar por la protección de la misma, según lo establecido en el Artículo 2 de la Constitución Política de la República de Guatemala.

Como parte de dicha protección a la seguridad, emana la seguridad digital, la cual no goza de un reconocimiento como tal y de forma expresa, pero el cual no es motivo de exclusión, ya que el derecho es dinámico y, dado el avance tecnológico que se encuentra en constante evolución, surge el derecho a la seguridad digital, como un derecho humano inherente a la persona, que forma el rubro de la quinta generación de derechos, y consiste en la protección a la seguridad que goza una persona dentro del ámbito tecnológico y espacial dentro del mismo. Es decir, la protección de los datos e información privada de las personas que utilizan el internet y la web dentro del territorio guatemalteco.

De esta forma se evidencia la importancia del reconocimiento a la protección de la seguridad de las personas; por ende, la seguridad de los datos de las personas en el espacio cibernético, en el uso de plataformas o aplicaciones del internet, en especial los datos sensibles de las mismas.



2.1 La seguridad y sus divisiones más comunes

Como se ha expuesto anteriormente, la seguridad de la que goza toda persona; es un deber del Estado de Guatemala, el brindar la respectiva protección, abarca múltiples tipos de seguridad, las cuales pueden ser:

Seguridad individual: Como individuo, una persona goza de la protección a su integridad, sus pensamientos, sus creencias y formas de ser. Para lograr el desarrollo íntegro de la misma es importante que se sienta segura.

Seguridad social o colectiva: Es la clase de seguridad que se refiere a la protección de la persona dentro de un grupo de personas, y a su vez, la protección del grupo de personas como un conjunto.

Seguridad familiar: La cual consiste en la protección al núcleo familiar, al derecho de toda persona a sentirse protegida dentro de un vínculo en un conjunto de personas.

Seguridad vial: Esta división de la seguridad, hace referencia al derecho que tiene toda persona que se encuentra circulando dentro de un área peatonal o automovilística. Es uno de los derechos más violentados que existe en la población guatemalteca.

Seguridad ambiental: Consiste en el derecho a gozar de un ambiente limpio, agradable y sano, así como la protección de la flora y fauna que existe en el territorio guatemalteco.



Seguridad física: Esta división de la seguridad consiste en la protección a la integridad física de una persona, el respeto a la privacidad, a su cuerpo, así como de su honor.

Seguridad digital: División de la seguridad de reciente creación derivada de la evolución tecnológica y el mundo digital, que consiste en la protección de los datos e información que se encuentran en un espacio digital. Así como de los programas, códigos, aplicaciones y sistemas que se desprendan del mismo y el uso cotidiano de las redes sociales.

Seguridad laboral: Es el derecho que tiene toda persona de poder desarrollarse en el ámbito laboral, es decir, la protección de la que goza una persona en el ejercicio de su actividad física, remunerada y bajo relación de dependencia. Así como la seguridad del empleador al recibir el servicio o trabajo contratado.

Seguridad ciudadana: Es una de las divisiones de la seguridad, de mayor importancia, la cual, consiste en la protección de los derechos civiles y políticos que emanan del reconocimiento que realiza el Estado de Guatemala, para con las personas nacidas dentro de la República como de las personas que han obtenido su naturalización.

Seguridad jurídica: Consiste en la seguridad que brinda la normativa jurídica dentro del territorio nacional, deriva de la protección y garantía que posee una persona al confiar en las leyes que protegen sus derechos inherentes y derechos humanos. Es decir, la certeza y seguridad que transmite el efectivo cumplimiento de la normativa jurídica en relación con la protección de las personas.

Seguridad patrimonial: Es el derecho que tiene toda persona a poseer un patrimonio, a tener objetos que posean un valor pecuniario. Dicha seguridad se refiere a la protección que tienen los monumentos, lugares turísticos, la bandera y todos los sitios que sean de índole pública, así como la protección de los bienes privados y derechos reales que tiene una persona, derechos reales y los bienes públicos.

Seguridad Política: Esta seguridad se enfoca en proteger los derechos de una persona a ser electa y elegir, el poder participar de la representación del poder público, así como el de las personas que forman un colectivo denominado partido político, los cuales gozan del derecho de protección a sus derechos individuales y colectivos.

Como hemos observado, la seguridad como derecho, que posee una persona, abarca gran parte de la esfera en la vida de la misma.

La seguridad digital, la cual se desprende de la mencionada ciencia, aún no posee un cuerpo taxativo que haga mención de su protección como tal, más, la existencia de los derechos humanos marca un camino al respeto y conservación del mismo.

2.2 Antecedentes del derecho a la seguridad digital

Derecho a la seguridad: Como primer antecedente del derecho de seguridad encontramos en la revolución francesa, la figura de la seguridad como tal, reconocida en la Declaración de los Derechos del Hombre y del Ciudadano de 1789, en el artículo 2, tras incansables luchas contra la desigualdad, opresión y esclavitud que adolecía el

vivir de nuestros antepasados. La lucha por el poder, entre otros factores de la historia hace que la lucha, en ese entonces, termine con la mencionada declaración. Marca una pauta para la protección y seguridad de la integridad de la persona, así como la de los derechos humanos inherentes a la persona. Continúa su reconocimiento con el Artículo 3 de la Declaración Universal de los Derechos Humanos, en la cual se reafirma el valor que posee tal derecho inherente a la persona humana, conformado por un bloque humanístico que robustece la protección a la misma.

Con las referidas declaraciones de los derechos humanos se crean antecedentes de suma importancia, los cuales son:

Derechos de primera, segunda y tercera generación. Dado que el tema de los rubros de los derechos humanos nos llevaría a un análisis extensivo sobre los mismos, se limitará en esta investigación a resaltar los aspectos importantes del tema en mención.

Integrados por los bloques humanísticos de derechos, y plasmados los primeros en el Pacto Internacional de Derechos Civiles y Políticos en 1966, conforman los derechos de Primera Generación, reconocidos como tal y antecedentes, no solo del derecho a la seguridad, sino de la libertad, igualdad, justicia, etc.

El segundo bloque de derechos humanos, conocidos como: Segunda Generación de Derechos Humanos. Se encuentran reconocidos de forma expresa en el Pacto Internacional de Derechos Económicos, Sociales y Culturales, pertenecientes al rubro de derechos humanos que buscan la protección del área personal como del derecho

colectivo, por ejemplo: El derecho al sindicato, derecho al trabajo y remuneración. Los cuales forman un antecedente de la división de la seguridad como derecho humanístico.

En cuanto a los derechos de tercera generación, consisten en la protección de los derechos que emanan de los de primera y segunda generación; son resultado de la aplicación y defensa de este rubro humanístico, tales como la paz, la democracia y la libertad social.

Derechos humanos de cuarta generación: Consisten en el conjunto de derechos humanos que surgen con la sociedad de la información, “tienen su sustento en la necesidad de asegurar el acceso a las tecnologías de la información y la comunicación a todos los individuos. “¹⁴

Son un rubro de derechos humanos que han surgido con el avance y desarrollo de la humanidad, es por ello que su reconocimiento como tal, aún no ha sido oficializado, a diferencia del conjunto de derechos de primera, segunda y tercera generación, cuya coyuntura los obligó a dejarlos plasmados de forma textual. Sin embargo, que no exista un reconocimiento expreso u oficial como tales derechos, no significa que no existan, que no estén presentes en la humanidad; sería en vano negarlos, ya que el avance tecnológico se encuentra en constante avance, desarrollo y perfeccionamiento implementando la modernización digital.

¹⁴ MARTÍNEZ VILLALBA, Juan Carlos. **Riofrío la cuarta ola de derechos humanos los derechos digitales** [http://CESOP-IL-72-14-DerHumaCuartaGeneracion-310817%20\(2\).pdf](http://CESOP-IL-72-14-DerHumaCuartaGeneracion-310817%20(2).pdf). Pág. 18. (Consultado el 06 de diciembre de 2022).

La revolución industrial: Es un antecedente importante del derecho a la seguridad digital, ya que con ello se encamina la sociedad a una época de transformación económica, social y tecnológica que se inició en el siglo XVIII. La actual tecnología tiene sus inicios en maquinaria básica, como lo fue para el cultivo en sus primeros pasos al desarrollo.

El incremento de PIB per cápita permite el avance hacia una era moderna y tecnológica, las cuales se habían estancado durante siglos.

La expansión de las actividades comerciales, modifica la forma de vivir de la población, y surge la necesidad de que las maquinarias se adapten a un trabajo más rápido, funcional y eficiente.

Como último rubro encontramos los derechos humanos de quinta generación. Comprenden los derechos nacidos por el avance tecnológico mundial, y se dirigen a herramientas tecnológicas, como máquinas, artefactos, *software* inteligente, etc. Encontramos a la seguridad digital, comprendida en la última clasificación, dado su mención en varias páginas de internet, sin tener un reconocimiento oficial, más que la utilizada por la Comisión de Derechos Humanos del Estado de México en la presentación de diapositiva denominada: "Teoría General de los Derechos Humanos"¹⁵.

¹⁵ CODHEM. **Teoría general de los derechos humanos**. https://sgg.edomex.gob.mx/sites/sgg.edomex.gob.mx/files/files/Comite_de_Etica/3%20TEORIA%20GENERAL%20EN%20MATERIA%20DE%20DERECHOS%20HUMANOS.pdf. Pág. 2 (Consultado el 06 de diciembre de 2022).

Si bien el reconocimiento como una clasificación de derecho humano oficial, es un factor importante, no podemos a partir de ello suponer la no existencia de tales derechos, ya que estos existen, no pueden excluirse porque son inherentes a la persona humana, así como las garantías que con ellas figuren, según lo establece el Artículo 44 de Constitución Política de la República de Guatemala.

2.3 Alcances del derecho a la seguridad digital

Los alcances logrados por las ciencias jurídicas y sociales, en relación a la regulación de las conductas humanas y los distintos bloques o rubros de los derechos humanos, representan un gran avance para el desarrollo integral de una persona.

Si bien el derecho a la seguridad digital, como derecho humano de quinta generación, no se encuentra regulado de forma expresa como tal, posee normas sociales que lo regulan y reglamentos internos creados por los servidores, aplicaciones y productos, lo cual, representa una base para la existencia de una futura legislación, ya que dichas normas toman de ejemplo un derecho ordinario. Aunque la mencionada normativa sea de carácter social, evidencia la importancia de mantenerlas dentro de un límite permisivo para el uso de las mismas.

Entre los alcances que abarca el derecho a la seguridad digital encontramos, como primer punto, la protección del espacio de navegación, el cual se encuentra restringido a través de normas de conductas cibernéticas, por ejemplo: *Facebook*, tiene la política actual de la no creación de cuentas o usuarios falsos, para ello ha implementado el

reconocimiento facial. Protección a los datos en plataformas y medios sociales: dicha protección abarca el cifrado de documentos, archivos y fotos, así como chats en los cuales se han adoptado medidas, como la implementación de un código QRL.

La seguridad digital representa para las empresas un derecho importante, ya que entre más seguro se sienta el internauta, navegante o usuario, mayor es el uso que se le da a una plataforma, sistema o red social.

En cuanto a las normas jurídicas en Guatemala, se implementó una reforma al Código Penal de Guatemala, el cual se abordará en su apartado respectivo.

El derecho a la protección de la seguridad digital, representa también la protección al derecho de libertad de expresión, puesto que las normas sociales y conductuales, que regulan la actividad dentro del medio cibernético, protegen, también al derecho de expresarse de forma escrita, gestual, visual o verbal ante los demás usuarios de la red y de forma recíproca.

El derecho de seguridad digital abarca la protección al derecho de identidad, el cual se beneficia de la protección que brindan las normas conductuales y reglamentarias, que brindan el uso de las plataformas, servidores y medios digitales, ya que, con las prohibiciones que estipulan, logran establecer un control de parámetros que impiden el mal uso de la información brindando protección al derecho de privacidad, que consiste en el derecho que tiene toda persona de tener su espacio personal; a la protección que goza una persona dentro del espacio cibernético por medio del cual la seguridad digital

juega un papel importante, puesto que entre más seguros se encuentren los datos de una persona en un programa, dispositivo u sistema, mayor será el uso y consumo del mismo.

Protección al derecho de personalidad, es uno de los derechos que mayor importancia posee, derivado del robo de identidad, sumado al robo de datos personales para el mal uso y destino de los mismos. Las plataformas como *Facebook* y *WhatsApp* tienen políticas internas para evitar la usurpación de la identidad, así como la creación de perfiles falsos, con la finalidad de erradicar el ciberbullying, robo de datos, robo de identidad. Para ello han implementado el uso de código QR para brindar una mayor protección.

Como hemos observado, en el desarrollo de la presente investigación, podemos apreciar que pese a no estar reconocida la seguridad digital, como un derecho humano de quinta generación, está ya se encuentra siendo protegida y aplicada por plataformas o medios digitales, sin embargo, es preocupante que sean medios electrónicos privados los que tengan en consideración tal protección, y, por su parte, en la actualidad no existen campañas informativas, como un mínimo, por parte de alguna institución Estatal que hable acerca de la misma y el uso de las redes privadas virtuales, que pueden ser de protección o amenaza.

Los entes estatales deben sumarse a la regulación, control y autorización de las redes privadas virtuales, ya que no puede negarse su existencia, la cual es independiente a la

vulneración que pueda producir a un derecho humano que se encuentre reconocido como tal.

2.4 Breve análisis de la normativa jurídica en Guatemala relacionada a la Seguridad digital de las plataformas.

A continuación se abordaran algunos ejemplos de artículos que dan cavidad a la seguridad digital y las redes privadas virtuales dentro del ámbito del sector público.

2.4.1. Registros de la propiedad

El Registro de la Propiedad regulado en el Artículo 1124 del Decreto Ley 106, mismo que abarca un libro entero de la misma ley; es una de las entidades estatales, que se encuentra en constante modernización, y para efectos de la presente, será utilizado para ejemplificar el constante desarrollo tecnológico.

El Artículo 4 del Decreto 30-2005 Reglamento del Registro de la propiedad, establece: “Todos los libros que se lleven en los Registros, serán rayados y foliados de manera uniforme. Cuando éstos se lleven en forma electrónica o similar, deberán cumplir los mismos requisitos en cuanto a su uniformidad, inalterabilidad, seguridad y certeza jurídica, así como su publicidad por los medios idóneos.”¹⁶. Podemos observar en el anterior ejemplo, que la normativa nos habla de un registro electrónico, en el cual se

¹⁶ JIMENEZ SUCESORES, AYALA. **Reglamento de los registros de la propiedad**. Guatemala: Ed. Ayala jimenez sucesores. 2021.

podría utilizar un bloqueador de red privada virtual pública, o en su defecto, una red privada virtual y de seguridad, entre otros principios. El artículo 40 del mismo reglamento establece "... modernización... e instalación de nuevas tecnologías".¹⁷ Actualización al que está afecto el registro de la propiedad, en el cual se puede incluir la protección al derecho de seguridad digital, así como su normativa en cuanto al uso, control, permisión y prohibición de las redes privadas virtuales, como método efectivo, para protección de la información de los usuarios.

Si bien el articulado es determinado, podemos concluir, en este caso, que en el registro de la propiedad no existe una normativa específica, que regule la seguridad digital y el uso, control y prohibición o aceptación de las redes virtuales privadas. Sin embargo, no impide la modernización tecnológica, la cual puede desencadenar en una adición al reglamento para lograr la protección a la seguridad digital y de esta forma lograr el desarrollo íntegro de las personas, así como, su adaptabilidad al mundo de la tecnología.

Como ente encargado del registro, resguardo, anotación y control de información personal en relación a las propiedades de sus habitantes, la cual es sensible, es de importancia que cuente con una seguridad digital propicia, que proporcione total confianza a los guatemaltecos en relación a la conservación, resguardo y manejo de la misma, mediando la actualización de dichos datos e incorporando una base de datos tecnológica, actualizada y confiable.

¹⁷ Jimenez Sucesores, Ayala. **Reglamento de los registros de la propiedad**. Guatemala. Pág. 9.

2.4.2 Registro mercantil

Es el encargado del registro de los comerciantes, así como las atribuciones que dicha institución señala en el Código de Comercio de Guatemala, Decreto 2-70 del Congreso de la República de Guatemala.

Para efectos de la presente investigación, utilizaremos el Reglamento del Registro Mercantil, contenido en el Acuerdo Gubernativo Número M. de E. 30-71. Si bien el antes mencionado registro, no posee una legislación específica para la regulación al derecho de seguridad digital, así como el uso de las redes privadas virtuales, ha adoptado en su página electrónica, la modernización de consultas, trámites en relación al comercio y toda la actividad que se desprende de ello.

Actualmente, cuenta con un apartado denominado “econsultas” cuya función es proporcionar información acerca del formulario a presentar y pasos a seguir, modernizando así al registro. Sin embargo, observamos la ausencia de control en el uso de las redes privadas virtuales, o en su defecto, la prohibición que hable acerca de las VPN, que no puedan utilizarse con dicho servidor. Notamos la ausencia de información acerca de la seguridad digital y la falta de medidas de seguridad, ya que es una página que cuenta con funciones básicas.

El Registro mercantil podría sufrir una mejora electrónica en su servidor web, es decir, una modernización, tal cual está sucediendo con el Registro de la Propiedad y la Superintendencia de Administración Tributaria (SAT).



2.4.3 Superintendencia de Administración Tributaria

La Superintendencia de Administración Tributaria (SAT), es una entidad descentralizada estatal con competencia y jurisdicción en todo el territorio nacional. Cuya función principal es la recaudar, controlar y fiscalizar los tributos internos y todos los tributos que gravan el comercio exterior, administra el sistema aduanero, entre otras funciones, según lo establece el Artículo 1 y 3, inciso a), de la Ley Orgánica de la Superintendencia de Administración Tributaria, Decreto Número 1-98 del Congreso de la República de Guatemala.

Es decir, que dicho ente, tendrá a cargo la fiscalización en cuanto a la recaudación de los tributos estatales se refiere, como función principal. Ello conlleva a que la recaudación deba hacerse de una forma ágil, sencilla y rápida; además, debe ser cómoda para los usuarios administrados.

Todo ello nos lleva a visitar el sitio web de la Superintendencia de Administración Tributaria, la cual a partir del año 2018 se ha modernizado de una manera impresionante, dado que esta cuenta con sistemas de planillas integradas para efectuar las declaraciones de impuestos correspondientes. Pero, al igual que otro ente su enfoque en la creación del usuario, es superior al enfoque de protección de los datos de los mismos. A diferencia de otros entes, al ingresar al usuario, esta tiene predeterminado un mensaje en que indica que no se debe compartir los datos de acceso con ninguna persona. Aparte de este signo de seguridad, no encontramos una advertencia o información del uso de las redes privadas virtuales, que las permita o las

prohíba, que informe o detalle el impedimento de las mismas, al igual que no cuenta con la información del derecho a la seguridad digital.

Dentro del Acuerdo del Directorio Número 007-2007 de la Superintendencia de Administración Tributaria, que contiene el Reglamento Interno de la misma, podemos encontrar en su Artículo 25, numeral 12, una de las funciones del Superintendente, lo cual es: “asignar los recursos humanos, financieros y materiales que requiera el Tribunal Administrativo y Aduanero para su funcionamiento”, articulado que abre una brecha para lograr la modernización tecnológica y las redes privadas virtuales.

Dentro de los considerandos del reglamento antes mencionado, encontramos los principios que motivan la modernización y seguridad de las entidades estatales. En este caso, aunque la Superintendencia de Administración Tributaria se haya actualizado en manejo y recaudación de tributos, ha obviado la seguridad del usuario y sus datos, dado que podría accederse a las cuentas de los mismos a través de una red privada virtual.

La actualización a la emisión de facturas es un gran paso al control de los tributos de los usuarios, los cuales pueden ser invertidos para la implementación de las aplicaciones seguras que permitan una navegación libre y sin preocupaciones.

Sin embargo, con la reciente ola de multas fantasmas, la entidad ha perdido credibilidad, lo cual se convierte en un factor que vulnera la certeza jurídica del ente y deja desprotegido al usuario, tal como hemos observado en los correos electrónicos que simulan una dirección de la entidad, en la cual se reclama el pago de una sanción

económica interpuesta contra el usuario; desconociendo el registro de la dirección IP de la cual proviene, es decir, que una persona podría estar utilizando de forma ilícita una función de las redes privadas virtuales, consistente en programar una IP no estática y cambiante.

Existen normas jurídicas en Guatemala, que remiten a la digitalización de archivos, documentos y datos en relación al registro de las acciones humanas, sin embargo, estas no indican la forma en que serán protegidas, no indica el método para evitar que las amenazas que existen en la web vulneren los datos sensibles.

Sin embargo, cabe resaltar que el hecho de enfrentarse a la digitalización de los datos de los usuarios, pese a ser un gran reto, representa un avance como Estado, en cuanto a dirigirse a proporcionar un desarrollo integral de la persona; representando un reto, dado que el ser humano posee una naturaleza evolutiva. La búsqueda de la satisfacción personal hace surgir nuevas eventualidades positivas o negativas, de las cuales los entes de gobierno deben tomar en cuenta para su tratamiento oportuno.

CAPÍTULO III

3. Derecho humano de la seguridad digital de quinta generación y el derecho comparado.

El derecho comparado, es el método por medio del cual se somete a comparación la legislación de un Estado con la de otro, para encontrar posibles soluciones. El derecho de seguridad digital, como derecho humano correspondiente a la quinta generación, es un derecho nuevo, nacido de la modernización tecnológica y desarrollo de la misma, por ende su estudio, tipificación o análogo aún se encuentra en vías de reconocimiento o desarrollo, inclusive por parte de los países que actualmente son potencia mundial. La dificultad de tener un control sobre la protección de los datos de los usuarios es un hecho evidente; sin embargo, no es imposible la regulación del mismo.

Guatemala, como ente encargado del desarrollo de las personas, ha incluido la modernización tecnológica en lo que le es posible, iniciando con establecimientos educativos, centros de informáticos, uso de red y WIFI gratuitos cuya instalación se encuentra en los espacios públicos y recreativos, todo ello derivado de las tecnologías implementadas en otros estados.

El derecho comparado ha servido de modelo para el desarrollo e implementación de avances sociales, culturales, tecnológicos, informáticos, industriales, laborales y jurídicos. La sociedad guatemalteca actualmente desarrolla sus actividades cotidianas,

a través de métodos y mecanismos cibernéticos, que facilitan la realización de dichas actividades.

Todo este desarrollo, posee su surgimiento en otros estados que se han dedicado a la investigación científica y desarrollo de *software* y *hardware*, especializados para realizar las tareas que una persona física realizaría; países como Japón, China, Rusia, Corea, España, etc. Actualmente cuentan con máquinas inteligentes, que van desde distribuir una lata o frituras, hasta prendas, bebidas o inclusive sostener una conversación básica con una persona.

El desarrollo sistemático, tecnológico o informático de los mencionados países, proporciona una perspectiva de los múltiples resultados que pueden obtenerse derivados de las investigaciones científicas, cuyo objetivo primario es el desarrollo de la humanidad.

Las ciencias jurídicas no se encuentran aisladas de dicho desarrollo tecnológico, puesto que dentro de la esfera que engloba el procedimiento de avance social, encontramos figuras como: patentes, licitaciones, cotizaciones, normativas que autorizan el traslado de componentes o partes destinadas a la creación de un objeto a utilizar en el resultado de una investigación, inclusive los químicos que formarán parte de un proyecto, deben cumplir con la normativa jurídica que los tipifica dentro del Estado que los requiere.

En el caso de las VPN, el derecho comparado ha proporcionado una visualización a las funciones de seguridad que estas proporcionan, el buen uso de las mismas, así como la

autorización para operar dentro del espacio cibernético de un ente Estatal, bajo supervisión del mismo, que produce efectos positivos y negativos para los usuarios que navegan.

A continuación encontramos una breve visualización del uso de las redes privadas virtuales, así como los derechos humanos de quinta generación.

3.1 Breve Análisis de los derechos humanos de quinta generación

Es de conocimiento de las personas, que los derechos humanos se dividen en primera generación, segunda generación y tercera generación, los cuales comprenden derechos inherentes a la persona humana como libertad, igualdad, economía y asociación, entre otros. Sin embargo, pocos conocen la división de los derechos humanos de cuarta generación, pertenecientes a los derechos de los animales no humanos, así como los derechos humanos de quinta generación, que comprenden los derechos nacidos por el avance tecnológico mundial y se dirigen a herramientas tecnológicas como máquinas, artefactos, *software* inteligente, etc.

Encontramos a la seguridad digital, comprendida en la última clasificación brindada en múltiples páginas de internet, sin tener un reconocimiento oficial, más que la utilizada por la Comisión de Derechos Humanos del Estado de México, en la presentación de

diapositiva denominada: “Teoría General de los Derechos Humanos”.¹⁸ Si bien, el reconocimiento como una clasificación de derecho humano oficial, es un factor importante, no podemos, a partir de ello, suponer la no existencia de tales derechos, ya que estos existen y no pueden excluirse porque son inherentes a la persona humana, así como las garantías que con ellos figuran, según lo establece el Artículo 44 constitucional de Guatemala.

3.2 Derechos humano de seguridad digital y la normativa jurídica en México

La seguridad digital en Guatemala, como hemos expuesto en algunos ejemplares, no cuenta con una normativa específica, pero, sí cuenta con leyes que en su momento de análisis, darían cavidad a la implementación de reglamentos, entre otros, para la subsanación de tal laguna. En relación al tema en el caso de México, el cual es un país federado, es aún más difícil su codificación ya que una persona que desee estar actualizada en la materia, entre otras, además de leer todos los días el Diario Oficial de la Federación, deberá sumarle la lectura de las gacetas y periódicos oficiales de las 32 entidades federativas.

Pese a lo extenuante que conllevaría implementar la seguridad jurídica, México ha logrado ya, que la Comisión de Derechos Humanos del Estado de México en la presentación de diapositiva denominada: “Teoría General de los Derechos Humanos” haga uso de la referencia del derecho de seguridad digital, como derecho humano de

¹⁸ CODHEM. **Teoría general de los derechos humanos**. https://sgg.edomex.gob.mx/sites/sgg.edomex.gob.mx/files/files/Comite_de_Etica/3%20TEORIA%20GENERAL%20EN%20MATERIA%20DE%20DERECHOS%20HUMANOS.pdf. Pág. 2 (Consultado el 06 de diciembre de 2022).

quinta generación. Lo cual, aunque es un pequeño aporte, representa el inicio de un camino por el cual se realizan preguntas sobre la existencia de los mismos, cosa que en Guatemala, la mayoría de personas, incluso estudiantes, desconocen y no le dan la importancia que merece el constante cambio que sufren los derechos inherentes a la persona humana. Es más, representa un tema de conflicto en la actualidad en materia penal.

En México, se plantea la Ley General de Ciberseguridad, la cual conlleva el objetivo de hacer frente a los ciberataques, mediante el proyecto de decreto de un marco legal, regula la protección de la información y sanciona los delitos cibernéticos y aminora los riesgos o pérdidas por estos ataques.¹⁹

Si bien en México, no encontramos legislación que estipule, ya sea la seguridad digital o el uso de las VPN, podemos observar que contiene información variada acerca de la ciberseguridad, misma que no se encuentra lejos de parecerse a la seguridad digital.

La ciberseguridad en México, es un tema que está cobrando vida, dado el aumento de niños vulnerados bajo modalidades electrónicas que se ven reflejadas en el número de denuncias. Este es un tema que tiene en común el Estado de Guatemala. Cada día crece el número de casos de crímenes, delitos y faltas contra la integridad de los menores de edad que utilizan como medio ejecutor, un medio electrónico, o en su defecto, un dispositivo electrónico.

¹⁹ EthicsGlobal. **Legislación en ciberseguridad México.**<https://blog.ethicsglobal.com/legislacion-en-ciberseguridad-mexico-2020/> (Consultado el 06 de diciembre de 2022).

Durante el primer semestre del año en curso se han reportado 85,000 millones de ciberataques, equivalente al 40% de aumento en comparación del año pasado. De acuerdo con la compañía de Ciberseguridad *Fortinet*.²⁰ Es preocupante el alto porcentaje de hechos ilícitos cometidos a través de medios electrónicos y cibernéticos, que anula la intervención del estado en cuanto a la seguridad digital de las personas. Si bien, la ciberseguridad está compuesta de mecanismos de acción en contra de los posibles delitos, que ocurran durante la navegación en el internet o web, tanto esta como la seguridad digital, buscan la protección del usuario durante la navegación y antes de iniciada la acción delictiva.

En cuanto al sector justicia, la población mexicana y la guatemalteca tienen similitud en la afluencia de delitos comunes, ambos estados no han logrado la verdadera disminución de los mismos y del crimen organizado. La sociedad, sufre las consecuencias que emanan de la comisión de acciones ilícitas que afectan los hogares de las personas; por ende, las familias se ven afectadas por el impacto que producen los delitos y faltas, en la crianza de sus hijos, en especial de los menores de edad. Ejemplo de ello lo encontramos en los constantes asesinatos, homicidios y lesiones que dejan a dicho conjunto, sin un miembro dentro de las mismas.

La normativa mexicana busca regular el uso de las VPN, como medio o instrumento que sirve para la comisión de hechos ilícitos, iniciando con la focalización de la existencia las redes privadas virtuales, su uso, función, objetivos y forma de instalación; así como

²⁰ El economista. **México reprueba en ciberseguridad, según reporte de IQSec.** <https://www.eleconomista.com.mx/tecnologia/Mexico-reprueba-en-ciberseguridad-segun-reporte-de-IQSec-20220828-0002.html> (Consultado el 06 de diciembre de 2022).

la focalización de la existencia de derechos humanos que han surgido dentro de la navegación al momento que el usuario utiliza la web, el desarrollo de estos derechos humanos y su relación con la evolución tecnológica en cuanto al hardware, es decir, la forma corpórea que almacenara el software. Para ejemplificar lo anterior, encontramos los robots inteligentes, programas simuladores de conversaciones humanas conocidos mundialmente, como lo es Alexa y Siri incorporados en los *iPhone*.

3.3 Derechos humano de seguridad digital y la normativa jurídica en China

China es una potencia mundial, el lugar con mayor desarrollo tecnológico del cual la mayoría de esta tecnología llega al territorio guatemalteco para la reutilización del mismo, derivado de los distintos tratados internacionales de comercio suscritos por Guatemala.

La mayoría de sistemas de ciberseguridad, que guardan relación con la protección al derecho de seguridad digital, creados bajo normas sociales, reglamentarias y/o culturales, son desarrollados por estos mismos.

Lo más parecido a la seguridad digital en China, es la ciberseguridad, la cual contempla la prohibición de divulgar, dañar o manipular información personal de un individuo, sin consentimiento, muy parecido a lo estipulado en el Artículo 274 del Código Penal de Guatemala.

Dentro de los programas de las VPN, se acompañan indicaciones y normativa jurídica que avala la creación y autorización de las mismas. En Guatemala, las personas desconocen incluso la política que se desarrolla dentro del uso de las redes privadas y la seguridad digital.

El avance tecnológico en dicho país es abismal, por lo cual la ciencia va de la mano con lo antes mencionado, y por ende, no queda excluida la normativa jurídica, en especial por ser la encargada de regular y proporcionar las directrices, bajo las cuales se emplearán los avances de *software* y *hardware*, entre otras funciones propias de la informática. Tal intervención jurídica la observamos materializada a través del registro de patentes que hacen constar la autoría de tales avances, entre otras. Sin embargo, más que un avance, actualmente para dicha potencia representa una estrategia, es decir, el uso de la tecnología no se limita a proporcionar rapidez, a ser funcional y brindar herramientas eficaces para la elaboración de tareas simples y complejas, sino se visualiza emplear la misma para el uso de operaciones que puedan llegar incluso a la ejecución de coordenadas, órdenes e incluso organizar las funciones básicas de un país.

En el caso de Guatemala, en comparación con el avance tecnológico chino, opta por difundir y emplear un avance mínimo, se limita a la ejecución de herramientas básicas que proporcionan los programas, sin mencionar que varias de estas se predeterminan por el propio programa que se instala en un ordenador, o bien que se descarga a través de la internet; haciendo que la vulneración a la seguridad jurídica de las personas en Guatemala se convierta en un hecho más, que en un supuesto, sumado el hecho de

que los órganos, instituciones, ministerios y demás entes encargados de la protección de la sociedad y el cumplimiento de sus derechos, se encuentran sumergidos en una ola de corrupción que impide enfocarse en la solución oportuna de tal vulneración.

Guatemala, emplea actualmente dentro de sus órganos y entes estatales el uso de la tecnología, como un medio de comunicación entre el usuario y el mismo; ejecuta acciones básicas de compartimiento de datos, resoluciones, notificaciones, citaciones y demás, limitándose a una función básica, mientras China contempla el avance robótico como un medio de servicio y agilización de las funciones estatales y privadas, evidenciando así el avance tecnológico de dicho país. Asimismo, muestra un interés en la regulación de las redes privadas en cuanto al uso correcto de estas, su relevancia en la protección de datos de los usuarios.

En relación al uso de las redes privadas virtuales, los habitantes de China poseen conocimiento de su existencia, así como de las funciones básicas de las mismas e incluso estas se encuentran prohibidas, ya que pueden servir como un medio evasivo de restricciones en cuanto a la censura de información compartida por el gobierno chino a sus habitantes, sin mencionar que simula una ubicación distinta de la transmisión de datos originaria. Con ello, reforzamos la importancia que tiene el conocer, nombrar, prohibir o normas las redes privadas virtuales en Guatemala, en cuanto a su uso como forma de prevención y disminución de la comisión de delitos que derivan del mal uso de las VPN.

En el año 2017, China anunció a sus habitantes la prohibición del uso de VPN, durante 14 meses, ya que realizaría una depuración o limpieza de las conexiones de internet.²¹

Siendo esta una medida que posee sus efectos positivos y negativos, en el caso de los primeros, ayuda al gobierno de un país a mantener el orden de la información que se publica, dominio de los datos que registran, así como la protección de los mismos eliminando servidores y/o dominios maliciosos, pero cuyo efecto negativo conlleva a la centralización de datos, censura, bloqueo, mal uso de las VPN, dictaduras informáticas y privativas.

3.4 Derechos humano de seguridad digital y la normativa jurídica en Rusia

Rusia, es una potencia mundial la cual, cuenta con un desarrollo tecnológico superior al país guatemalteco, cuyas empresas se encuentran profesionalizadas en el tema de cibercrimen; condición que el actual presidente ha impuesto para que operen dentro del territorio del país. También es notorio que, así, como se profesionalizan las empresas de seguridad digital, existe irónicamente gran cantidad de *hackers* que tienen como objetivo el pentágono, las infraestructuras críticas y esenciales, ciberdelincuentes cuyo fin es la recompensa económica.

Pese al avance que ha tenido, no ha mostrado mayor interés en regular el derecho a la seguridad digital, o en su defecto, normar el uso de redes privadas, ya que dentro de los servidores de VPN públicos encontramos IP dinámicas del mencionado país, o, al

²¹ SOPHOS NEWS. **China prohíbe el uso de las VPN.** <https://news.sophos.com/es-es/2017/01/25/china-prohibe-uso-las-vpn/> (Consultado el 06 de diciembre de 2022).

menos ello era lo que se consideraba hasta el año dos mil diecisiete, en el cual, bajo el mandato de Vladimir Putin, siguiendo el ejemplo del gobierno de China, prohíbe el uso de las redes privadas dentro del país como método de seguridad de los datos de los usuarios. Sin embargo, es notorio que dicha finalidad ocupe el último puesto en la lista de prioridades de tal gobierno, observando así, la limitante y vulneración de los derechos inherentes a la persona humana.

Las redes privadas representan un arma de doble filo para los Estados, ya que, por un lado, son sinónimo de seguridad de navegación anónima y, por el otro, sirven de medio para materializar delitos cibernéticos, estafas, robos de identidad, y método opresivo de información.

El Estado, como ente representativo de un país en relaciones exteriores, no se encuentra excluido dentro de los sujetos que puedan emplear con finalidades análogas las VPN, como se demuestra en las múltiples notas que pretenden ser informativas en páginas cibernéticas o diarios no oficiales cibernéticos, cuya veracidad no se entra a dirimir, pero sirven, como precedente de la actualidad que viven los usuarios dentro del territorio de los mismos.

La limitante informativa es un elemento importante en la forma de controlar las acciones y percepciones de las personas, utilizada como herramienta de opresión por parte de un gobierno, para evitar la pronunciación de la población sobre un tema que causa dolencia, molestia o afección a los intereses colectivos, lo que conlleva a una aceptación tácita de las acciones gubernamentales, las cuales verán su efecto positivo

o negativo en su materialización y no en su forma subjetiva, en pocas palabras, la población catalogará las acciones de un gobierno como buenas o malas, hasta que sean notorios los efectos de las mismas, imposibilitando su depuración a través del pronunciamiento cuando estas se encuentran en la etapa de planeación o el proceso de creación. Otra forma análoga de emplear una red privada, es depurando la información que se encuentra en los sitios web, limitando el uso de *proxys*, datos y programas que se encuentran en la internet, logrando de forma el monopolio y el imperio del espacio cibernético.

El ente Estatal busca su independencia, aun en el espacio virtual, como es el caso de Rusia, con la Ley de Internet Soberano para construir la *RuNet*,²² la cual pretende desconectar al país del resto del servidor global, conseguir su propia red autónoma, sus propias normas, y por ende, con el contenido que el gobierno permita compartir bajo el ideal de la depuración o eliminación de los sitios con contenido ilegal.

Evidenciando, así, la importancia de tomar acción en cuanto al tema de la normativa de las redes privadas en cuanto a su uso, control, restricción o aceptación de las misma, ya sea por parte del gobierno de Guatemala o por los usuarios del territorio antes mencionado, en cuanto a la importancia de conocer la existencia, buen uso de la mismas; así como proporcionar el nombre de los servidores que proporcionan y garantizan la correcta programación y configuración de las redes privadas, a emplearse para la protección de los datos de las personas dentro de la circunscripción territorial.

²² WIRED. **Rusia aumenta, silenciosamente, su maquinaria de censura en internet.** <https://es.wired.com/articulos/rusia-mecanismos-de-censura-en-internet> (Consultado el 06 de diciembre de 2022).



CAPÍTULO IV

4. Protección a la seguridad digital y las redes privadas virtuales

El usuario de la República de Guatemala, sea un ente, persona física o jurídica, que emplee las funciones de una VPN, las cuales, siguiendo su naturaleza, pueden ser:

Conectarse a una red pública a través de un túnel cifrado de datos, utilizando para ello un “disfraz” de la IP (*Internet Protocol*), la cual es una dirección única que identifica a un dispositivo, para proteger los datos personales, bancarios y privados.

La creación de una red local que puede darse desde cualquier parte del mundo; facilitando así el acceso desde cualquier lugar y protegiendo la ubicación del usuario para evitar seguimiento de sus acciones electrónicas.

Acceso de contenido que se encuentra bloqueado o censurado en determinados países, simulando con ella estar en otro que cuente con la autorización debida. Lo cual es útil al momento de consultar noticias, programas o material cuyo fin sea impedir su divulgación a la sociedad, porque conlleva un fin dañino y evasión al acceso a la información pública.

El uso de las funciones adecuadas de las redes privadas, al momento de navegar en el espacio cibernético proporciona una amplia seguridad de los datos de los usuarios, sin obviar, que la utilización no adecuada de las mismas conlleva al medio para la

materialización de delitos. El Estado, como principal garante de los derechos inherentes al ser humano, independientemente del ámbito en el que se desarrollen, tiene la obligación de velar por el respeto de los mismos y, por ende, implementar las herramientas, programas, funciones, registros y demás que ayuden a su garantía.

Una de las principales formas de protección a la seguridad digital de los usuarios, además del uso correcto de las VPN, encontramos en su análogo, una navegación privada, conocida también como: modo incognito, ventana privada o en su defecto navegación segura; misma que consiste en ocultar datos primarios que sirven para la navegación e identificación del usuario en la web, para su seguridad; sin embargo, esta no oculta cookies, ni historial visitado por el usuario durante su navegación.

Continuando con la protección del usuario en el espacio cibernético y la seguridad digital, como un derecho que emana del desarrollo tecnológico de la humanidad, encontramos los antivirus, son los más conocidos actualmente por el usuario ya que son las principales defensas de los sistemas operativos que brindan protección básica, sirven de escudo contra amenazas que ocasionan la pérdida de datos, documentos, imágenes e incluso la alteración de los mismos, sin mencionar el daño al archivo o enlace que los contiene, en comparación con una red virtual privada, estos no ocultan o simulan un espacio geográfico distinto al que se opera o ejecuta el programa, posee una desventaja en contra de los virus o amenazas de reciente surgimiento, que va acompañada del desarrollo de la humanidad, el tecnológico y por ende de los Estados.

El modo seguro, el cual consiste en ingresar a las funciones básicas del *software* y *hardware* de las computadoras y /o dispositivos, para ejecutar programas de depuración, modificación y configuración de herramientas defectuosas, o bien, evitar la ejecución de programas en segundo plano que contengan archivos dañados o infectados por los denominados virus o amenazas.

Un usuario con conocimientos básicos de computación puede acceder a este modo, ejecutando así las herramientas como *Word*, *Excel*, entre otras para realizar sus actividades cotidianas o acceder al modo seguro con internet. El modo seguro con acceso internet limita las funciones de desarrollo y ejecución de las cookies y elementos de una página web, impidiendo, así, que se ejecuten estos con finalidades de acceso ilícito hacia los datos sensibles y privados que los usuarios tengan en resguardo en sus dispositivos electrónicos.

Actualmente las páginas web universales, protegen los datos de los usuarios a través de los llamados corta fuegos, cuya semejanza con las VPN es muy parecida, ya que estos poseen la función de servir como pasarela en la internet, funcionan como estaciones que verifican la autenticidad de los datos que se procesan en el ciberespacio, impidiendo así el paso de aquellos cuya finalidad sirva de amenaza para la seguridad del usuario, sin embargo, al ser estos un lenguaje de informática poseen un filtro estricto el cual a diferencia de una red privada, que puede configurarse para bloquear determinados datos o páginas, el corta fuegos es más estricto en cuanto a la información que deja pasar para poder acceder a un sitio web, es decir uno funciona

como aplicación, programa o adhesión y el otro funciona a través del lenguaje de programación e informática o comandos.²³

4.1 Plataformas virtuales como medio masivo informativo

En la actualidad existen múltiples medios de comunicación que van desde los tradicionales panfletos, cronogramas, esquemas, carteles, cartas, entre otros. Hasta los actuales que consisten en las redes sociales, como el uso de *Facebook*, *Instagram*, *Snapchat*, *WhatsApp*, etc. Los cuales son de gran utilidad para dar a conocer las funciones correctas del uso de las Redes Privadas Virtuales, así como el compartir el conocimiento sobre el derecho a la seguridad digital y la importancia de su protección.

Encontramos otros medios visuales, que involucran a los jóvenes dentro de las campañas informativas, que el Estado de Guatemala puede impulsar, como lo son los *Challenge*, los *TikToks*, y *Snapchat*.

Las aplicaciones de última generación, que se actualizan de manera constante y sin pausa alguna, representan un reto en cuanto a su regularización dentro del marco jurídico de un ente estatal; sin embargo este puede ser una herramienta funcional en cuanto al esparcimiento de la información del buen uso de las redes privadas virtuales, cuya función adicional respaldaría a la entidad en la lucha contra los delitos

²³ IBM. **Firewalls**. <https://www.ibm.com/docs/es/i/7.1?topic=options-firewalls>. (Consultado el 06 de diciembre de 2022).

cibernéticos. Dentro de las plataformas virtuales, encontramos una protección inherente, como sistema de defensa contra las amenazas, que pueden vulnerar la red que compone una web o aplicación.

Para ejemplificar lo expuesto con anterioridad, iniciaremos con el navegador *Chrome*, siendo uno de los navegadores con mayor afluencia en cuanto a su uso y reconocimiento por contener una gran cantidad de sitios web, enlaces, sitios o espacios cibernéticos de toda clase de contenido, el cual se ha visto en la necesidad de incorporar dentro de sus extensiones y configuraciones el uso de una VPN para resguardar los datos de sus usuarios; entonces surge una interrogante: ¿Por qué, si las VPN son un arma de doble filo, son utilizadas para la protección de datos? Así como un balón de fútbol tiene como función primaria, ser utilizado como instrumento para ser golpeado con los pies; servir para un torneo y divertir, puede que una persona lo utilice como arma o con fines delictivos.

De igual forma sucede con las redes privadas, cuya función principal ha sido abordada durante el desarrollo de la presente investigación. Esta puede variar si el cibernauta le destina una función análoga para la que fue diseñada y programada.

El navegador denominado Opera, es otra plataforma web o navegador que encierra un conjunto de elementos, configuraciones, extensiones y demás para la protección de datos contenidos dentro del conjunto informático que lo engloba, el cual ha tomado el riesgo, ya que ha introducido dentro de su configuración primaria el uso de cortafuegos, que impiden que los anuncios publicitarios introduzcan amenazas dentro de los

ordenadores, así como el uso de las redes privadas electrónicas, permitiendo al usuario la configuración de las mismas o, en su defecto, el uso de las incorporadas de forma predeterminada, es decir, incorpora una lista de redes privadas para utilizarse sin necesidad de conocimientos avanzados en programación.

Los entes estatales, argumentan no poseer el suficiente presupuesto para poder realizar campañas informativas que ayuden a la prevención de los medios de comisión de delitos, como lo son las redes privadas virtuales. Sin embargo, pese a que en cierta proporción dicho argumento puede ser verídico, no es de desconocimiento para las personas, que, a través de la grabación de un video y el uso de datos, por sencillos que sean, puede reproducirse un mensaje masivo.

En conclusión, el Estado de Guatemala debe explotar las redes sociales y medios electrónicos, para el esparcimiento de conocimiento que ayude a mejorar a las personas, para hacer un aporte en el crecimiento integral de cada ciudadano, habitante o residente de la república de Guatemala.

4.2 Formas de regularización jurídica para uso, control y regulación de las redes privadas virtuales en Guatemala

En Guatemala se tiene la falsa creencia de que el único modo de supervisar o regular un comportamiento, circunstancia o situación, es a través de una norma constitucional o superior, lo cual resulta totalmente falso, ya que existen otras alternativas que proponen una solución incluso más factible que iniciar un proceso legislativo.

En el ámbito administrativo existe una variedad de disposiciones de carácter normativa jurídica, que conforman el conglomerado de normas enfocadas a la prohibición o autorización de determinadas conductas, productos, situaciones, licencias, espacios, etc.

Dentro del mencionado conglomerado encontramos los reglamentos, que vienen incorporados dentro de una aplicación o programa, contienen normas jurídicas en relación con la autoría de creación de los mismos, así como las consecuencias que emanan de su incumplimiento. Asimismo, describe la normativa internacional que protege las ganancias lícitas que se perciban por su creación y distribución, por ejemplo, regula la venta del *software* sin la autorización correspondiente, el compartimiento de sus datos internos derivados de la misma causa.

Contienen normas de uso insertadas como sugerencias, en caso de ser no ser acatadas, ejecuta acciones de bloqueo para el despliegue de las funciones que se pretenden violentar, observando así uno de los métodos jurídicos y electrónicos para el control de las mismas.

En el ámbito social, la regularización en su uso y control, emana de los bloqueos internos que posee el software de instalación. En cuanto al uso de las VPN, en relación al ente estatal de Guatemala, encontramos las normas consuetudinarias emanadas de las costumbres y derechos humanos del hombre, por ejemplo: el respeto a la igualdad, a la privacidad, la tolerancia y la autoría. Encontramos una regularización intrínseca en

relación al tema, es decir, toda persona con práctica de valores frenará su actuar en cuanto al mal uso de la herramienta.

La regularización jurídica y la regularización, pese a ser dos términos semejantes, abordan un fin distinto, ya que el primero regula de forma coercitiva el actuar de una sujeto emanado del estado, mientras, el segundo, carece de dicha fuerza para regular circunstancias que pueden afectar al usuario, porque derivan de un ente comercial o una persona jurídica. Además de contener prohibiciones, regula funciones básicas que ayudan al usuario o las personas acatar determinadas directrices.

Una circunstancia regulada puede dirigir a las personas al comportamiento correcto de la acción a realizar, evitándose así la comisión de faltas o delitos, es decir, la regularización de una circunstancia o acción no siempre encuadra un comportamiento atípico e ilícito, puede abordar directrices y acciones a ejecutar para la obtención de un mejor resultado, mientras la regularización jurídica prevé la tipificación de una acción que puede desencadenar en la materialización de un delito o falta. También aborda lo relacionado con la sanción a imponer por el incumplimiento o desacato a la misma.

Tanto la regulación en su concepto básico, como la regularización jurídica son de interés estatal, puesto que ambas comparten la finalidad de brindar seguridad a las personas, cualquiera que sea la materia a las que afectará o abordará. Siendo la segunda la de mayor importancia, ya que es una obligación impuesta a los Estados, que consiste en proporcionar protección a los derechos humanos de las personas en cualquiera de las etapas de su vida.

El abordaje anterior sirve de base para comprender la importancia de acciones direccionadas a la prevención del mal uso de las redes privadas, como principal tema de esta investigación, las cuales pueden representar un avance tecnológico y la disminución de la comisión de delitos, utilizando estas como medios para la ejecución de encubrimiento de actos u omisiones delictivas.

Entre las soluciones más factibles que predominan para el abordaje de la problemática planteada en la presente investigación, encontramos:

- Circulares administrativas
- Reglamentos
- Normas jurídicas específicas

Proponen una solución al problema planteado de una forma efectiva, eficaz y eficiente. Ya que no necesitan de proceso riguroso para su creación, sin embargo, es necesario el proceso administrativo-judicial para revestirse de fuerza coercitiva, necesaria para imponerse y sancionarse ante la materialización de las conductas tipificadas como antijurídicas e ilícitas. Las soluciones propuestas con anterioridad tienen una mayor probabilidad de adaptación al avance tecnológico y cibernético, puesto que al no estar sujetas a un procedimiento jurídico riguroso, pueden actualizarse de manera continua, rápida y eficiente, respondiendo, así casi de inmediato ante las problemáticas derivadas de las constantes actualizaciones en todos los ámbitos de vida de las personas, contribuyen al desarrollo de los seres humanos en el ámbito social, cultural y jurídico,

puesto que las directrices a su vez que guían, educan a la población en cuanto a los temas afectos.

4.2.1 Circulares Administrativas

Son medios de notificación entre el órgano superior administrativo y los órganos inferiores, por medio del cual el primero le comunica directrices, cuyo objeto es producir efectos dentro de la administración, denominados como circulares internas.²⁴

En el ámbito administrativo judicial, una circular conlleva una comunicación de relevancia para la ejecución de procedimientos que deberá realizar el órgano al cual se dirigen.

La mayoría de ciudadanos e incluso trabajadores de las instituciones estatales pasan por alto la importancia de estas, ya que dentro de la jerarquía jurídica ocupan un nivel inferior a una norma jurídica. Pero todo ello no hace menos relevante su papel dentro de la sociedad, en especial en relación al tema de las redes privadas electrónicas.

Por medio de las circulares de carácter administrativas-judiciales, se ha logrado implementar las mejoras dentro de una institución u órgano estatal, que van desde una modernización de amueblados, hasta la modernización del sistema de cómputo de los mismos, cayendo así en el punto más relevante a abordar en relación a estas, ya que a

²⁴ Enciclopedia jurídica. **Circular administrativa**. <http://www.encyclopedia-juridica.com/d/circular-administrativa/circular-administrativa.htm>. (Consultado el 06 de diciembre de 2022).



través de una solicitud realizada, a través de una correspondencia básica se logra un procedimiento de compra-venta de equipo, el cual abarca herramientas, *software*, *hardware* de un procesador.

El Organismo Judicial de Guatemala, que representa un claro ejemplo, como órgano encargado de la administración de justicia, no puede quedar vedado de la actualización electrónica del cual se ve afecto el país, ejecutando la misma a través del Centro de Informática y Telecomunicaciones,²⁵ mismo que a través de una circular administrativa instala y provee a sus dependencias el respectivo soporte.

El CIT del mencionado órgano provee, además de equipo de cómputo, apoyo e instalación de *software*, para el óptimo desarrollo de las funciones del ordenador, proveyéndolo de protección contra amenazas al sistema por medio del cual realiza sus funciones. Sin embargo, pese a contar con el antes mencionado centro y dichas funciones, este órgano no puede compararse con la actualización cibernética que ha logrado el Ministerio de Finanzas Públicas, ya que este también ejecuta actos administrativos utilizando las plataformas electrónicas que tienen como base instrucciones giradas por medio de circulares internas.

Posterior a la adquisición de las mejoras tecnológicas, se requiere que el órgano superior gire instrucciones para la instalación y la utilización de la mejora asignada, todo

²⁵ Organismo Judicial. Manual de normas y procedimientos del centro de informática y telecomunicaciones–CIT-http://www.oj.gob.gt/files/Ley%20Acceso%20a%20la%20Informacion%20Publica%20Articulo%2010/6/Manual_Aprobado_de_Procedimientos_CIT.pdf. (Consultado el 06 de diciembre de 2022)

ello se da a través de una circulara administrativa; evidenciándonos que estas poseen un alto nivel de importancia para lograr la regulación interna del uso, control, autorización o prohibición del uso de las VPN dentro de los servidores de los órganos e instituciones estatales para garantizar el derecho a la seguridad digital de los usuarios.

4.2.2 Reglamentos

Los reglamentos, son disposiciones que rigen las circunstancias internas dentro del órgano administrativo que rigen a cada uno de ellos de forma descentralizada. Poseen una supremacía judicial sobre una circular administrativa, la cual es una disposición interna que gira alrededor de una orden para instalación o uso de determinada herramienta, mejora electrónica u objeto.

Regulada en la Constitución Política de la República de Guatemala, en el Artículo 183 literal e, como una función, que le corresponde al Presidente de la República de Guatemala para el cumplimiento de las leyes, sin que esto altere su naturaleza para las que fueron creadas, suponen una solución administrativa judicial para la protección de los datos de los usuarios dentro del Estado de Guatemala, porque puede dirigirse a dictaminar el uso de una red virtual de forma privada, es decir, autorizaría el uso de las VPN que cuente con las últimas actualizaciones, y medidas de seguridad requeridas para el óptimo funcionamiento que garanticen la protección durante la navegación.

Desde la perspectiva jurídica, los reglamentos dictaminados por el presidente de la República de Guatemala, pueden normar la utilización o prohibición del uso de la VPN

durante su navegación. Dicha disposición no sería contraria a las normas ordinarias, que posee el ente estatal, bajo su gobierno y directriz, ya que estas dentro de sus preámbulos o motivos expositivos, así como su cierre, dejan abierta la posibilidad de las mejoras que conlleven al desarrollo humano en cualquier de sus ámbitos, siendo uno de esos ámbitos, el desarrollo dentro de la esfera informática y cibernética.

Observamos entonces la escala jurídica que gira en torno al uso de las redes privadas dentro de la circunscripción territorial dentro de Guatemala, iniciando mediante la acción de órdenes leves en relación al uso de las funciones de las VPN, como su inclusión mediante un reglamento que admita o prohíba su ejecución mediante la navegación del espacio cibernético de dominio estatal.

Debe tenerse en cuenta que una solución no está revestido de sinónimo de perfección, es decir, que posee el defecto humano de utilizar la misma para fines análogos, como se ha observado en legislaciones y entes estatales internacionales, que utilizan la misma para privar a su población de determinada información que los afecte o favorezca.

4.2.3 Normas jurídicas específicas

Consiste en la creación de la norma jurídica, en su proceso legislativo, establecido en los Artículos del 174 al 181 de la Constitución Política de la República de Guatemala, denominado como proceso legislativo.

La diferencia entre una norma jurídica y una norma jurídica específica, es que la primera aborda acciones u omisiones de carácter general. Estas pueden contemplar una situación de argumento de analogía o *simdili* jurídica que se materializa cuando “la resolución de un caso o la interpretación de una norma fundándose en el espíritu de un ordenamiento positivo o en los principios generales del derecho”,²⁶ y la segunda, es creada para contemplar un determinado hecho u acto jurídico que afecta a la sociedad en general.

Una de las soluciones a la problemática planteada en esta investigación, es la creación de una norma jurídica que regule el uso, control y prohibición de las redes privadas en Guatemala, las cuales pueden ser utilizadas como medios para la comisión de delitos y su vez la protección del derecho a la seguridad digital.

La solución antes descrita, es por naturaleza la de mayor efectividad e importancia, puesto que a través de la misma, se logra el buen uso de la herramienta, como medio, como aplicación, como extensión o cualquiera que sea su modalidad correspondiente al desarrollo tecnológico de su época.

El uso de las redes privadas virtuales, como tal no posee una tipificación que se enfoque únicamente en el objeto de la misma, que la regule para su ejecución del objetivo para el cual fue creado, pero, sí, cuenta con normativa jurídica análoga en

²⁶ CABANELLAS DE LAS CUEVAS, Guillermo. Diccionario jurídico elemental, nueva edición y comentada. Buenos Aires: Ed.Heliasta, 1993.

relación a los efectos que produce la utilización de estas, para la comisión de delitos, tal como fue analizado en el apartado correspondiente de la investigación.

El conglomerado de normas jurídicas existentes en el territorio guatemalteco es basto; sin embargo, este se enfoca más en los efectos producidos, por acciones y omisiones de carácter ilícitas, que en su prevención y abolición.

Esta normativa es de carácter genérico; contempla la universalidad de acciones delictivas o sus efectos.

Para ejemplificar lo antes descrito, encontramos la actualización más reciente en materia judicial, la cual, es la implementación de bandejas electrónicas, que sirven como receptores de comunicación entre los órganos e instituciones estatales, que van desde creación de perfiles, suscripciones por correo electrónico, hasta la creación del casillero electrónico, siendo este último el más llamativo, puesto que no solo representa el desarrollo y alcance tecnológico que se implementa, para la facilitación de las notificaciones.

También representa el desarrollo de la humanidad encaminada a la dignificación de la persona humana, puesto que la finalidad de su creación es la facilitación al acceso de las actuaciones que se envíen a través de este, de forma igualitaria para todos los habitantes; creado a través de los decretos 12-2022 y 13-2022, ambos relacionados a la adhesión de las mejoras tecnológicas universales.



La creación de una norma jurídica específica, que desarrolle el funcionamiento de las redes privadas virtuales de forma detallada y explícita, proporcionaría al usuario un aporte educativo, preventivo y consciente en cuanto al uso correcto de las funciones de estas.

Si el usuario conoce que es una VPN, puede proteger su identidad durante su navegación, proporcionando oportunidad y seguridad para realizar denuncias administrativas, jurídicas y sociales, sin temer por las represalias que conlleva está, en el actual entorno social. En cambio, si el usuario descubre que puede ocultar su identidad, y no existe normativa alguna que prohíba tal situación, o la regule, navegará y dará usos análogos que pueden conllevar a la comisión de hechos delictivos.

Mediante el uso de protección de identidad y uso de una IP dinámica, utilizando una red privada virtual de forma regulada, castigando los actos que deriven de su uso malicioso, pero implementando un bloqueo dentro de la VPN autorizada, se lograría el correcto funcionamiento para el que fueron destinadas, sin caer en una norma que regule el efecto malicioso producido por el uso análogo.

A través de una norma jurídica específica, que contemple el uso correcto de las redes privadas virtuales, así como, la prohibición de las que representen una amenaza a la seguridad jurídica de los usuarios, puede obtenerse más que un castigo, por la omisión o comisión de hechos y actos delictivos con posibilidad de quedar impune; un verdadero efecto rehabilitador a través del anonimato, puesto que una VPN controlada y regulada, permitiría a los usuarios realizar comentarios, denuncias, aportes y seguimientos

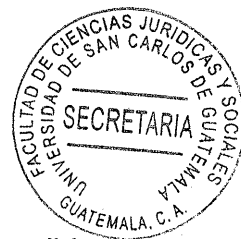


informativos, para la prevención de la comisión de un hecho o acto delictivo, así como la desarticulación de bandas criminales y grupos delictivos o narcomenudeo.

El Estado de Guatemala, puede utilizar como ejemplo, para la creación de una normativa jurídica, las directrices que acompañan los servidores, las aplicaciones o extensiones al momento de utilizar una VPN.

Es un hecho, la existencia e incorporación de las redes privadas virtuales, en Guatemala, como una aplicación, extensión, programa o adhesión; producto de la constante evolución de la tecnológica, *software*, *hardware*, espacios cibernéticos, entre otras. Así como el surgimiento de los derechos humanos de quinta generación, en especial la seguridad digital, que en resumen, y cuya finalidad de esta propuesta es dar a conocer la existencia de las redes privadas virtuales, o en su idioma natal, *Virtual Private Network* por sus siglas en inglés: VPN.

Evidenciando, la necesidad de su regulación para su uso, control, autorización o prohibición para ser empleadas como herramientas de protección, a los derechos inherentes a la persona humana, ya sea por parte de entidades estatales, personas jurídicas individuales o colectivas, durante la navegación en el mundo electrónico y cibernético, para la prevención de los actos u omisiones ilícitas emanadas de la conducta consciente y humana, mediante circulares administrativas jurídicas y reglamentos creados por el presidente de la República, perfeccionándose a través del medio idóneo, consistente en el proceso legislativo, culminante en una norma judicial específica en su materia.



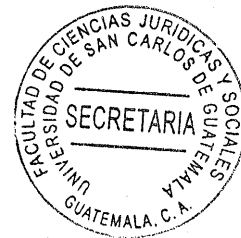
Debido al constante desarrollo tecnológico que envuelve a la humanidad, es imposible delimitar con antelación los actos, omisiones, o hechos jurídicos que sean realizados por las personas, para la comisión de delitos dentro del mundo cibernético, con efectos materiales y palpables, sin embargo, esta delimitante, no es causal o justificativo para la comisión de un hecho ilícito, tanto, para los Estados, como para las personas individuales y jurídicas.



CONCLUSIÓN DISCURSIVA

La vulneración al derecho de seguridad digital, como derecho humano de quinta generación, se da por el uso ilícito de las Redes Privadas Virtuales, como medios permisivos, y la falta de regulación jurídica por parte del Estado de Guatemala, al no cumplir con la obligación establecida, en el Artículo 2 de la Constitución Política de la República de Guatemala, como garante de la obligación de proteger el derecho a la seguridad, por ende, a la seguridad digital de las personas que residen dentro del territorio de la República.

El desarrollo de la humanidad, es un acontecimiento imparable e impredecible, del cual, se ha desprendido el desarrollo de la tecnología, como instrumento de comunicación, trabajo, conexión, descubrimiento, entre otros; por lo que el Estado de Guatemala, deberá implementar o incrustar dentro de sus conocimientos básicos, el manejo del desarrollo cibernético, dentro del cual, el uso correcto de las redes privadas virtuales (*Virtual Private Network* - VPN), debe ser público, y replicado dentro del territorio, así como su regularización, en cuanto a la prohibición de aquellas, que puedan convertirse en un núcleo de surgimiento de medios, para la comisión de delitos, así como dar a conocer, las que brinden seguridad, confianza y protección a los datos de los usuarios; de esta forma, garantizar la protección al derecho de seguridad digital, como derecho humano de quinta generación en Guatemala.





BIBLIOGRAFÍA

ACADEMY. **Qué es un malware troyano guía definitiva.** <https://www.avast.com/es-es/c-trojan> (consultado el 06 de diciembre de 2022).

CABANELLAS DE LAS CUEVAS, Guillermo. Diccionario jurídico elemental, nueva edición y comentada. Buenos Aires: Ed.Heliasta, 1993.

CODHEM. **Teoría general de los derechos humanos.** https://sgg.edomex.gob.mx/sites/sgg.edomex.gob.mx/files/files/Comité_de_Etica/3%20TEORIA%20GENERAL%20EN%20MATERIA%20DE%20DERECHOS%20HUMANOS.pdf. Pág. 2 (consultado el 06/12/2022).

Digital guide ionos. **Direcciones IP: todo lo que debes saber.** <https://www.ionos.es/digital-guide/servidores/know-how/direccion-ip/> (Consultado el 5 de diciembre de 2022).

El economista. **México reprueba en ciberseguridad, según reporte de IQSec.** <https://www.eleconomista.com.mx/tecnologia/Mexico-reprueba-en-ciberseguridad-segun-reporte-de-IQSec-20220828-0002.html> (Consultado el 06 de diciembre 2022).

Enciclopedia jurídica. **Circular administrativa.** <http://www.encyclopedia-juridica.com/d/circular-administrativa/circular-administrativa.htm> (Consultado el 06 de diciembre de 2022).

EthicsGlobal. **Legislación en ciberseguridad México.** <https://blog.ethicsglobal.com/legislacion-en-ciberseguridad-mexico-2020/> (Consultado el 06 de diciembre 2022).



GoDaddy. **Qué es una app, para qué se utiliza y qué tipos existen**
<https://es.godaddy.com/blog/que-es-una-app-y-para-que-se-utiliza/> (Consultado el 5 de diciembre de 2022).

GONZÁLEZ MORALES, Alexandro. **Redes privadas virtuales**. Universidad Autónoma del Estado de Hidalgo, Instituto de Ciencias Básicas e Ingeniería, Pachuca, Hidalgo.

IBM. **Firewalls**. <https://www.ibm.com/docs/es/i/7.1?topic=options-firewalls>. (Consultado el 06 de diciembre de 2022).

JIMENEZ SUCESTORES, AYALA. **Reglamento de los registros de la propiedad**. Guatemala: Ed. Ayala jimenez sucesores.2021.

KASPERSKY. **Qué es una dirección IP: definición y explicación**.
<https://latam.kaspersky.com/resource-center/definitions/what-is-an-ip-address>
(Consultado el 5 de diciembre de 2022).

KYOCERA. **8 tipos de virus informáticos que debes conocer**. <https://www.kyocera documentsolutions.es/es/smarter-workspaces/insights-hub/articles/8-tipos-virus-informaticos-debes-conocer.html> (Consultado el 5 de diciembre de 2022).

MALWARE. **Todo acerca de malware**. <https://es.malwarebytes.com/malware/>
(Consultado el 5 de diciembre de 2022).

MARTÍNEZ VILLALBA, Juan Carlos. **Riofrío la cuarta ola de derechos humanos los derechos digitales** [http://CESOP-IL-72-14-DerHumaCuartaGeneracion-310817%20\(2\).pdf](http://CESOP-IL-72-14-DerHumaCuartaGeneracion-310817%20(2).pdf). Pág. 18. (Consultado el 06 de diciembre de 2022).

Organismo Judicial. **Manual de normas y procedimientos del centro de informática y telecomunicaciones –CIT-**. [http:// www.oj.gob.gt /files/Ley%20Acceso%20a%20la %20Informacion%20Publi ca /Articulo %2010/6/Manual_Apro bado_ de_Procedimientos_ CIT.pdf](http://www.oj.gob.gt/files/Ley%20Acceso%20a%20la%20Informacion%20Publica/Articulo%2010/6/Manual_Aprobado_de_Procedimientos_CIT.pdf). (Consultado el 06 de diciembre de 2022).

SOPHOS NEWS. **China prohíbe el uso de las VPN**. <https://news.sophos.com/es-es/2017/01/25/china-prohibe-uso-las-vpn/> (Consultado el 06 de diciembre de 2022).

Tecinnova. **Hacker de sombrero negro, blanco y gris**. <https://www.tec-innova.mx/hackers-de-sombrero-negro-blanco-y-gris/> (Consultado el 5 de diciembre de 2022).

Wikipedia. **Hacker seguridad informática**. [https://es.wikipedia.org/wiki/Hacker_\(seguridad_informática\)](https://es.wikipedia.org/wiki/Hacker_(seguridad_informática)) (Consultado 5 de diciembre 2022).

WIRED. **Rusia aumenta, silenciosamente, su maquinaria de censura en Internet**. <https://es.wired.com/articulos/rusia-mecanismos-de-censura-en-internet> (Consultado el 06 de diciembre de 2022).

Legislación:

Constitución Política de la República de Guatemala. Título I La Persona Humana, Fines y Deberes Del Estado, Capítulo Único, (1986).

Declaración de los Derechos del Hombre y del Ciudadano. 1789.

Código de Comercio de Guatemala. Decreto 2-70 del Congreso de la República de Guatemala.



Código Penal. Decreto número 17-73 del Congreso de la República de Guatemala
1973

Reglamento de los Registro de la Propiedad. Título I, Capítulo I, De los Registros.
2017