UNIVERSIDAD PANAMERICANA
"Sabiduría ante todo; adquiere sabiduría"

Facultad de Ciencias Jurídicas y Justicia

Licenciatura en Ciencias Jurídicas y de la Justicia

Efectos producidos en la propiedad por la suplantación digital en Guatemala y el Derecho Comparado

(Tesis de Licenciatura)

Ernesto Francisco Herrera Castillo

Guatemala, septiembre 2022

Facultad de Ciencias Jurídicas y Justicia
Licenciatura en Ciencias Jurídicas y de la Justicia

Efectos producidos en la propiedad por la suplantación digital en Guatemala y el Derecho Comparado

(Tesis de Licenciatura)

Ernesto Francisco Herrera Castillo

Guatemala, septiembre 2022

Para los efectos legales y en cumplimiento a lo dispuesto en el artículo 1°, literal h) del Reglamento de Colegiación del Colegio de Abogados y Notarios de Guatemala, **Ernesto Francisco Herrera Castillo,** elaboró la presente tesis, titulada **Efectos producidos en la propiedad por la suplantación digital en Guatemala y el Derecho Comparado.**

AUTORIDADES DE UNIVERSIDAD PANAMERICANA

M. Th. Mynor Augusto Herrera Lemus
Rector

Dra. Alba Aracely Rodríguez de González
Vicerrectora Académica

M. A. César Augusto Custodio Cóbar
Vicerrector Administrativo

EMBA. Adolfo Noguera Bosque
Secretario General

FACULTAD DE CIENCIAS JURÍDICAS Y JUSTICIA

Dr. Enrique Fernando Sánchez Usera

Decano de la Facultad de Ciencias Jurídicas y Justicia

Guatemala, 07 de mayo de 2022

Señores Miembros
Consejo de la Facultad de Ciencias Jurídicas y Justicia
Universidad Panamericana
Presente

Estimados señores:

Tengo el agrado de dirigirme a ustedes haciendo referencia a mi nombramiento como **tutor** del estudiante: Ernesto Francisco Herrera Castillo, ID: 000032986. Al respecto se manifiesta que:

a) Brindé acompañamiento a la estudiante en referencia durante el proceso de elaboración de la tesis denominada: "**Efectos producidos en la propiedad por la suplantación digital en Guatemala y el Derecho Comparado".**

b) Durante ese proceso fueron sugeridas correcciones que realizó conforme los lineamientos proporcionados.

c) Habiendo leído la versión final del documento, se establece que el mismo constituye un estudio serio en torno al tema investigado, cumpliendo con los requerimientos metodológicos establecidos por la Facultad de Ciencias Jurídicas y Justicia para esta modalidad académica.

En virtud de lo anterior, por este medio emito **DICTAMEN FAVORABLE** para que se continúe con los trámites de rigor.

Atentamente,

LICENCIADO
Julio Raúl Mazariegos Pérez
ABOGADO Y NOTARIO

Licenciado Julio Raúl Mazariegos Pérez

Abogado y Notario.

Guatemala, 27 de junio de 2022

Señores Miembros
Consejo de la Facultad de Ciencias Jurídicas y Justicia
Universidad Panamericana
Presente

Estimados señores:

Tengo el agrado de dirigirme a ustedes, haciendo referencia a mi nombramiento como revisor metodológico de la tesis del estudiante Ernesto Francisco Herrera Castillo, ID 000032986, titulada Efectos producidos en la propiedad por la suplantación digital en Guatemala y el Derecho Comparado. Al respecto me permito manifestarles que, la versión final de la investigación fue objeto de revisión de forma y fondo, estableciendo que la misma constituye un estudio serio que cumple con los requerimientos metodológicos establecidos por la Facultad de Ciencias Jurídicas y Justicia para esta modalidad académica.

En virtud de lo anterior, por este medio emito DICTAMEN FAVORABLE para que se continúe con los tramites de rigor.

Atentamente,

Omiria Ludmila Ruiz Sanchinelli
Asesor

Ludmila Ruiz Sanchinelli
Abogada y Notaria

Lic. Domingo Sirineo Yojcom Mendoza
ABOGADO Y NOTARIO

En la ciudad de Guatemala, el día veinte de septiembre del año dos mil veintidós, siendo las quince horas, con veinte minutos yo, **DOMINGO SIRINEO YOJCOM MENDOZA**, Notario, número de colegiado veintiocho mil doscientos dieciséis (28216), me encuentro constituido en la primera avenida diez guión ochenta y siete zona diez, Edificio Torre Viva, oficina seiscientos uno, nivel seis, soy requerido por **ERNESTO FRANCISCO HERRERA CASTILLO**, de treinta y ocho años de edad, soltero, guatemalteco, Ingeniero en electrónica, de este domicilio, quien se identifica con el Documento Personal de Identificación (DPI), con Código Único de Identificación (CUI) número un mil seiscientos cincuenta y uno, treinta y nueve mil novecientos, cero ciento uno (1651 39900 0101), extendido por el Registro Nacional de las Personas de la República de Guatemala, quien requiere mis servicios profesionales con el objeto de hacer constar a través de la presente **DECLARACIÓN JURADA** lo siguiente: **PRIMERO:** El requirente, **BAJO SOLEMNE JURAMENTO DE LEY**, y enterado por el infrascrito notario de las penas relativas al delito de perjurio, DECLARA ser de los datos de identificación personal consignados en la presente y que se encuentra en el libre ejercicio de sus derechos civiles. **SEGUNDO**: Continúa declarando bajo juramento el requirente: i) ser autor del trabajo de tesis titulado: "**Efectos producidos en la propiedad por la suplantación digital en Guatemala y el Derecho Comparado**"; ii) haber respetado los derechos de autor de las fuentes consultadas y reconocido los créditos correspondientes; y iii) aceptar la responsabilidad como autor del contenido de la presente tesis de licenciatura. No habiendo nada más que hacer constar, finalizo el presente instrumento en el mismo lugar y fecha de inicio treinta minutos después, la cual consta en una hoja de papel bond tamaño oficio, impresa en ambos lados, que firmo y sello, a la cual le adhiero los timbres para cubrir los impuestos

correspondientes que determinan las leyes respectivas: un timbre notarial del valor de diez quetzales con serie BF guión cero novecientos veinte mil ciento veinte (BF-0920120) y un timbre fiscal del valor de cincuenta centavos con número de registro nueve millones doscientos veinte mil ochocientos cinco (9220805). Leo íntegramente lo escrito al requirente, quien, enterado de su contenido, objeto, validez y demás efectos legales, la acepta, ratifica y firma con el Notario que autoriza. **DOY FE.**

f)_____

ANTE MÍ:

Lic. Domingo Sirineo Yojcom Mendoza
ABOGADO Y NOTARIO

UNIVERSIDAD PANAMERICANA
"Sabiduría ante todo; adquiere sabiduría"

Ref. O.I. 183-2022
ID 000032986

ORDEN DE IMPRESIÓN DE TESIS DE LICENCIATURA

Nombre del Estudiante: **ERNESTO FRANCISCO HERRERA CASTILLO**
Título de la tesis: **EFECTOS PRODUCIDOS EN LA PROPIEDAD POR LA SUPLANTACIÓN DIGITAL EN GUATEMALA Y EL DERECHO COMPARADO**

El Decano de la Facultad de Ciencias Jurídicas y Justicia,

Considerando:

Primero: Que previo a otorgársele el grado académico de Licenciado en Ciencias Jurídicas y de la Justicia, así como los títulos de Abogado y Notario, el estudiante ya mencionado, ha desarrollado el proceso de investigación y redacción de su tesis de licenciatura.
Segundo: Que tengo a la vista el dictamen favorable emitido por el tutor, Licenciado Julio Raúl Mazariegos Pérez de fecha 7 de mayo de 2022.
Tercero: Que tengo a la vista el dictamen favorable emitido por la revisora, Licenciada Ludmila Ruiz Sanchinelli de fecha 27 de junio de 2022.
Cuarto: Que tengo a la vista el acta notarial autorizada en la ciudad de Guatemala, el día 20 de septiembre de 2022 por el notario Domingo Sirineo Yojcom Mendoza, que contiene declaración jurada del estudiante, quien manifestó bajo juramento: *ser autor del trabajo de tesis, haber respetado los derechos de autor de las fuentes consultadas y reconocido los créditos correspondientes; y aceptar la responsabilidad como autor del contenido de su tesis de licenciatura.*

Por tanto,

Autoriza la impresión de la tesis elaborada por el estudiante ya identificado en el acápite del presente documento, como requisito previo a la graduación profesional.

Guatemala, 27 de septiembre de 2022.

"Sabiduría ante todo, adquiere sabiduría"

UNIVERSIDAD PANAMERICANA · FACULTAD DE CIENCIAS JURÍDICAS Y JUSTICIA · Dr. Enrique Fernando Sánchez Usera DECANO

Dr. Enrique Fernando Sánchez Usera
Decano de la Facultad de Ciencias
Jurídicas y Justicia

Nota: Para efectos legales, únicamente el sustentante es responsable del contenido del presente trabajo.

Dedicatoria

A Dios, que sin él nada de todo esto hubiera sido posibles. Y que gracias a su misericordia me dio las fuerzas de nunca rendirme, me puso a las personas indicadas en mi camino y me demostró que con la fe todo se puede lograr.

A mi papá y mamá, por su amor incondicional y quienes forjaron valores en mí, con su ejemplo. Son quienes creen en mis capacidades y me incentivan a siempre seguir adelante, sin su esfuerzo yo no sería la persona que soy hoy en día.

A mis hermanos, quien cada uno a su forma ha sido un pilar en mi vida y me han acompañado de buenos y malos momentos. Con quienes hemos reído y llorado, y de no ser por ellos yo no estuviera haciendo esto. Gracias Carol, porque, si no fuera por vos, nunca hubiera iniciado esta travesía.

A mi abuelita Carolina, la quien a pesar de todo me cuida, me da de comer, me acompaña, me busca, me quiere incondicionalmente, reza por mí, me ha dado todo lo que tiene, para que yo esté bien y que si no fuera por ella no sé dónde estaría.

A mi esposa, quien es el amor de vida y sin ella no hubiera formado mi propia familia, quien me motiva a seguir adelante y a sacar lo mejor de mí, quien me llena de ilusiones y que sin ella no tendría el hogar que hoy en día tengo.

A mis hijos, Ernesto, María Clara y Mateo, quienes son un regalo de Dios y hoy están con él cuidándonos.

A Sofí y Moni, quienes con su alegría, amor y nobleza llenan mis ojos de alegría y orgullo. Soy bendecido por verlas crecer y ver las grandes personas en la que se están convirtiendo.

A mi tío Victor por siempre estar presente, por su cariño y solidaridad incondicional.

A mi primo Victor porque ha sido como un hermano y quien también con su cariño, nobleza, consejos y ayuda siempre he podido contar. Y a su esposa Vannia por ser alguien muy especial y a quien quiero mucho.

A la Ja-ja y a mi tía Patty. Por ser fuente de amor y alegría, que Dios las tenga en su gloria.

A mis tíos, Liz, Vicky, Letty, Rosita, Chiqui. Quienes siempre me demuestran su amor y me dan fuerzas para seguir adelante.

A mi gran amigo Alvaro, quien conocí en este viaje y ha sido parte de él. Hemos vivido tanto que guarda un espacio muy especial en mi corazón.

A mis grandes amigos, Oscar, Alejandro, Marco, Ruth, Daniel, Nelson, Victor L, Danilo, Selvin, Raúl, Mishelle, Mauricio y Douglas L. Quienes siempre han sido parte de mi vida y de alguna forma siempre me han demostrado su cariño y me han apoyado a seguir adelante.

A mis suegros, cuñados, sobrinos, primos por ser parte de mi vida y compartir conmigo muchos momentos.

A todas las personas con las que he compartido en mi experiencia laboral y académica de Herrera Peñalba y Asociados, Banco GyT Continental, Cementos Progreso, Ingenio Magdalena, Conduent, Allied Global, Universidad Galileo y Universidad Panamericana. Porque han hecho cada momento inolvidable y han dejado huella en mi vida.

A mis amigos del Colegio Lehnsen, con los que compartimos mucho y hoy en día siempre seguimos en contacto y compartiendo.

A Memphis y Dani. Por siempre estar a mi lado y alegrarme los días cada vez que los veo.

Y a todas las personas que de alguna forma han sido parte de mi vida y con quienes hemos compartidos.

Índice

Resumen

Con el nacimiento del internet y los sitios web, en los años ochenta, y el surgimiento de las redes sociales, plataformas de ocio y las criptomonedas, en la actualidad, se han creado circunstancias que abren las puertas a los delincuentes, para que se valgan del uso de la tecnología, del internet y de ingeniería social, para engañar a los usuarios y vulnerar su patrimonio. Entre estos métodos se puede mencionar, el enviar correos electrónicos a los usuarios de internet haciéndose pasar por instituciones financieras, por ejemplo, el delincuente redacta correos electrónicos solicitando información sensible, como claves de acceso, con el objetivo de violentar la seguridad de las plataformas de la misma institución financiera que se encuentra simulando. O también, es muy común ver, que los delincuentes crean perfiles en redes sociales con nombres e imágenes que identifican a una institución de renombre, contactando a sus usuarios con el fin de engañarlos para que realicen transferencias de dinero o proporciones información como, credenciales de cuentas de correo electrónico o claves de sistemas de información.

La presente investigación determinó los efectos producidos en la propiedad de las personas, al ciberdelincuente suplantar su identidad. Para lograr esto, se determinó que delitos informáticos regula el derecho penal guatemalteco y que aspectos de la propiedad son vulnerados, también se

examinó como se abordan los delitos de suplantación de identidad digital en el Derecho Comparado y se relacionó como estos ciberdelitos afecta jurídicamente la propiedad de las personas en Guatemala.

Palabras clave

Suplantación. Identidad. Digital. Ciberdelito. Propiedad.

Introducción

En los últimos años, los sistemas tecnológicos como el correo electrónico, las redes sociales, los sistemas financieros, el uso de las criptomonedas y los servicios de pago electrónicos han hecho que el internet tenga mucho mayor alcance y gradualmente se ha convertido en una necesidad básica para las personas. Esto ha motivado a que se desarrollen nuevos métodos para la comercialización de productos y servicios, ha modernizado las plataformas para realizar transacciones financieras y ha creado activos digitales que representan valor para las personas. En consecuencia, ha dado apertura a que los delincuentes utilicen nuevos métodos para cometer acciones que tienen como fin dañar el patrimonio tanto de las personas físicas, como el de las instituciones públicas o privadas.

La presente investigación pretende determinar los delitos informáticos cubiertos en el derecho penal guatemalteco, qué aspectos de la propiedad pueden ser vulnerados por la comisión de estos, y cuál es el abordaje de la suplantación de identidad digital en el Derecho Comparado; con el fin de relacionar como el delito de suplantación de identidad digital afecta la propiedad de las personas en Guatemala. La relevancia de la investigación consiste en dejar un aporte personal y resaltar la realidad nacional de los daños que causa la suplantación de identidad en la propiedad de los guatemaltecos, con el propósito de hacer ver al legislador los métodos

actualmente utilizados para engañar a las personas a través de los medios tecnológicos utilizados hoy en día, para que estos sean considerados en el ordenamiento jurídico y de llegar estas situaciones al órgano jurisdiccional, no queden en impunidad.

Guatemala en el artículo 39 de la Constitución Política de la República, establece que el Estado debe de garantizar la propiedad privada como derecho inherente a la persona. El legislador, debe de estar consciente de la realidad y buscar soluciones para brindar certeza jurídica con el fin de proteger la propiedad de las personas y de las instituciones, para fomentar el crecimiento económico del país. La modalidad de investigación será el estudio de Derecho Comparado, se analizará la legislación guatemalteca y adicionalmente la legislación vigente de distintos países que cuenten con aspectos culturales, territoriales y sociales similares a lo contenido en Guatemala, como los son Costa Rica, República Dominicana, y Puerto Rico. Con la información recabada plantear las conclusiones determinando las diferencias y similitudes.

La investigación consiste en tres temas principales de los cuales el primero capitulo se abarca las generalidades de los ciberdelitos, los aspectos del patrimonio como la propiedad, el derecho de autor y la propiedad industrial, y que delitos son lo que vulneran el patrimonio. A continuación, en el segundo capítulo se revisa el Convenio de Ciberdelincuencia de

Budapest y cuáles son los ciberdelitos que aborda, también se examina el Código Penal de Puerto Rico, el de República Dominicana y el de Costa Rica, por encontrarse en el mismo territorio y se países en donde la población cuenta con mayor acceso al internet en comparación con Guatemala. Y, por último, el capítulo tres, el cual ejemplifica los métodos utilizados por los ciberdelincuentes y de que formas las acciones vulneran el patrimonio de las personas que residen Guatemala, relacionando las acciones con el Derecho Comparado.

Los ciberdelitos y el derecho de propiedad en Guatemala

Los ciberdelitos

Previo a utilizar la palabra ciberdelito era comúnmente emplear el termino delito informático, el cual inicia a ser utilizado aproximadamente en los años ochenta, y este tiene sus raíces de la frase en inglés *computer crime* que hacía referencia a acciones como estafas informáticas, el acceso sin autorización a los sistemas, la piratería de obras del ingenio, entre otros. La característica común en cada una de las acciones mencionadas anteriormente es la utilización de sistemas informáticos para su comisión.

Los sistemas informáticos están definidos como "todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa" (Council of Europe, 2001, pág. 4). Actualmente son empleados los términos ciberdelito, cibercrimen y ciberdelincuencia, en el ámbito penal, que tienen una connotación especifica de los delitos que nacen a la vida por el surgimiento redes interconectadas a nivel mundial denominado ciber espacio.

De acuerdo con Fernández Bermejo et al. (2020) se define ciberdelito como "todo ilícito penal llevado a cabo a través de medios informáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las

Tecnologías de la Información y la Comunicación o que tiene como fin estos bienes" (p. 28). Es decir, hace referencia a las personas que realiza una acción ilegal en el ciber espacio. La característica particular que marca la diferencia entre el termino delito y el termino ciberdelito, está dada porque los ciberdelitos no nacen a la vida o no podría existir su razón de ser sin el internet o las tecnologías de la información o comunicación (TIC). Los términos ciberdelitos o cibercrimen, son utilizados indistintamente en la doctrina y el termino ciberdelincuencia es el grupo de personas, organizadas o no, que cometen o intentan cometer ciberdelitos.

En otras palabras, se definirá el ciberdelito como la acción u omisión de un acto descrito en la normativa jurídica en contra del patrimonio de las personas, valiéndose de medios como el internet o las tecnologías de la información y comunicación con el propósito de vulnerar los bienes jurídicos protegidos por el Estado. La variedad de ciberdelitos que existen, normalmente son denominados en inglés y estos son nombrados de acuerdo con características particulares. Conforme la tecnología avanza los rasgos característicos gradualmente cambian y esto hace que surjan nuevos subtipos de ciberdelitos. No todos ellos estarán enmarcados el ordenamiento jurídico y al realizar estudios de derecho comparado no todos será denominados de la misma forma y existe la posibilidad que sus

verbos rectores varíen, ya que esto dependerá de la concepción e interpretación del legislador.

También es importantes mencionar, que hoy en día es muy común que se utilicen indistintamente los términos delitos informático y ciberdelitos. Aunque los ciberdelitos son una nueva generación de delitos y que cuentan con una perspectiva criminológica distinta, por razones como tener la facilidad de poderse llevar a cabo desde cualquier lugar, afectar a distintas personas simultáneamente y la dificulta de determinar desde que lugar se cometieron los hechos ilícitos. En cambio, los delitos informáticos estaban enfocados a actos realizados localmente, en una misma red y básicamente se utilizaba una computadora en el mismo sitio para afectar un sistema local donde solo había un afectado. Es decir, un delito informático es un subconjunto de los ciberdelitos. Pero, es común que las normas jurídicas aun tengan denominado como delitos informáticos, los actos ilícitos cometidos en el ciberespacio. Por la simple y sencilla razón que estas no son actualizadas, al mismo ritmo con que van surgiendo los avances tecnológicos. Y para efectos prácticos, es mejor tener claro que estos dos términos serán utilizados como sinónimos.

Son varias las dificultades que los ciberdelitos generan a la sociedad y al sistema de justicia; por ejemplo, determinar la ubicación de dónde provino el ataque, al ser estos cometidos en el ciberespacio, el cual se compone de

múltiples sistemas interconectado por medios de comunicaciones transnacionales en cascada uno tras otro, esto dificulta el rastreo del origen del ataque y desconocerlo generara incertidumbre para seleccionar la jurisdicción a la que se debe de acudir a promover la persecución penal.

Otro de los retos es, la complejidad para obtener pruebas concretas que sean suficientes y de relevancia para el proceso penal. Y, por último, pero no menos importante, es que, se ha visto que los métodos utilizados para cometer ciberdelitos están cambiando exponencialmente junto al crecimiento tecnológicos y el ordenamiento jurídico no es actualizado al mismo ritmo, por consiguiente, en la mayoría de los casos se encontrara que los actos cometidos no se encuentran tipificadas y esto no permitirá al juzgador determinar que sanciones son las que se debe de aplicar.

La propiedad, el derecho de autor y la propiedad industrial

Respecto a la propiedad es importante mencionar que esta fue consagrada entre los derechos fundamentales de los ciudadanos por la Declaración de los Derechos del Hombre y del Ciudadano de 1789, la cual fue redactada en Francia en la época de la revolución francesa, donde se produce un cambio político social basado, en la razón, igualdad y la libertad derrocando un régimen conformado por la nobleza, quienes eran la minoría y la revolución buscaba mejores condiciones para la mayoría de

las personas, la declaración es considerada una expresión concreta de la libertad. Posteriormente tras la segunda guerra mundial, donde se cometieron violaciones contra la libertad y la vida de las personas, surge la Declaración Universal de los Derechos Humanos la cual establece, “1. Toda persona tiene derechos a la propiedad, individual y colectivamente” (Asamblea General de la ONU, 1948). Múltiples tratados internacionales sirven como base fundamental en donde los Estados deben de enfocar fuerzas para proteger la propiedad ya que esta es un derecho inherente de las personas.

En Guatemala no se define específicamente el derecho de propiedad, pero de acuerdo con el artículo 39, de la Constitución Política de la República de Guatemala (1985), Se garantiza la propiedad privada como un derecho inherente a la persona humana. Toda persona puede disponer libremente de sus bienes de acuerdo con la ley. El Estado garantiza el ejercicio de este derecho y deberá crear las condiciones que faciliten al propietario el uso y disfrute de sus bienes. La Constitución identifica como derecho inherente de las personas y protegido por el Estado, la propiedad. También establece que es lo que persona puede hacer con su propiedad.

Además, al estar reconocido por la Constitución de la República de Guatemala como derecho humano, el Estado debe de garantizar las condiciones que faciliten el uso y disfrute de sus bienes, esto implica

brindar de certeza jurídica en caso la propiedad sea vulnerada por terceros, quien de haber sido citado, oído y vencido en juicio queda obligando a resarcir por daños y perjuicios causado por dicha vulneración y en este punto el Estado debe hacer uso de su poder coercitivo para hacer valer la sentencia que haya quedo firme. Esto va muy de la mano con lo que establece el Código Civil (Decreto Ley 106), "el propietario tiene derecho de defender su propiedad por los medios legales …" (artículo 468). La excepción a la regla referente a la protección de la propiedad por parte del Estado está dada el artículo 40, "En caso concretos, la propiedad privada podrá ser expropiada por tres razones utilidad colectiva, beneficio social o interés público debidamente comprobado" (Constitución Política de la República de Guatemala, 1985).

Es importante mencionar que la propiedad no es únicamente un atributo de las personas individuales o jurídicas. También existe la propiedad del Estado la cual esta descrita en 8 incisos en el artículo 121 de la Constitución Política de la República de Guatemala, en forma general establece que la propiedad también es constituida por el patrimonio del Estado. Es decir, de igual forma que las personas, el Estado tiene derecho al uso y el goce de bienes, por ende, se deben de considerar que los bienes que son susceptibles de estimación económica, información pública o privada como los secretos que se manejan bajo el resguardo de la ley, secretos de Estado. Estos al igual que cualquier bien son susceptibles de

vulneraciones y el mismo Estado debe de velar por resguardar y el uso adecuado de la información.

Al referirnos al derecho de autor, en Guatemala, establece que lo producido de la autoría de las personas es su propiedad, de acuerdo con el Código Civil (Decreto Ley 106), "El producto o valor de trabajo o industria lícitos, así como las producciones del ingenio o del talento de cualquier persona, son propiedad suya" (artículo 470). En este aspecto existen un sin fin de cosas que pueden venir de la imaginación de las personas, a las cuales se les puede realizar estimación pecuniaria con el propósito de determinar el valor que representa para el patrimonio. Si a esto, en algún momento se ven vulnerados, la perdida estará dada por el valor estimado más lo que representan los frutos futuros y los daños y perjuicios por el uso inadecuado.

El Decreto número 33-98 del Congreso de la República de Guatemala Ley de Derechos de Autor y Derechos Conexos, es la ley específica que regula los derechos de los autores de obras literarias y artísticas, de los artistas intérpretes o ejecutantes, de los productores de fonogramas y de los organismos de radiodifusión. Hay que tomar en consideración que la ley citada anteriormente fue concebida en 1998 y de nuevo grandes avances tecnológicos han sucedido desde ese momento, entre ellos se pueden mencionar lo que hoy en día se conoce como los *non fungibles tokens art*

(NFT art) que son obras de arte digitales que cuentan con un autenticador único y estos se venden en mercados digitales donde comúnmente las transacciones son realizadas por criptomonedas. Adicionalmente es importante recordar que esto funciona utilizando distintos sistemas de resguardan estas obras de arte y son susceptibles de ser vulnerados.

Otra rama de la propiedad es la propiedad industrial, en Guatemala se encuentra regulada por el Decreto número 57-2000, Ley de Propiedad Industrial, la cual tiene por objeto según el artículo 1 “la protección, estímulo y fomento a la creatividad intelectual que tiene aplicación en el campo de la industria y el comercio…” (Congreso de República de Guatemala, 2000). Esto abarca aspectos como las invenciones, marcas, nombres comerciales, signos distintivos, etc. Esta ley surge como parte del Convenio de Paris para la Protección de la Propiedad Industrial, en donde el Estado de Guatemala se compromete a promover los mecanismos necesario para resguardar los derechos mencionados anteriormente desde un punto de vista comercial. Y cumple con estándares internacionales de protección contemplados en el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio.

La propiedad industrial hace referencia a un sinfín de aspectos intangibles que son parte del patrimonio de las personas individuales y jurídicas, inclusive el Estado mismo. Se pretende que la ley proteja por ejemplo que

la marca sea registrada por una institución del Estado y esto permita que sea oponible ante terceros. Es decir, básicamente lo que se trata de hacer es que si una persona tiene una marca registrada esto prevenga que otra persona haga uso y lucre con esta, todo esto desde un ámbito comercial. Pero en la actualidad, es común ver que las personas tomen estos signos distintivos, como por ejemplo un emblema, el cual es un signo que distingue a una empresa y este fácilmente se puede copiar digitalmente y ser utilizado para engañar o disuadir a otra persona en un correo electrónico o en una plataforma publicada en internet denominada red social, con el propósito de cometer un acto ilícito.

Así mismo, la Ley de Propiedad Industrial (Decreto número 57-2000) establece, “el estado velará porque se establezcan medidas eficaces, prontas y eficientes contra cualquier actos u omisión infractora de los derechos de propiedad industrial, inclusive para prevenir dichas infracciones y disuadir nuevas infracciones” (artículo 178). Para hacer valer la proteccion del Estado de Guatemala u otros Estados, la propiedad debe de encontrarse registrada. Ya que de esta forma se gozara de los derechos como, el uso exclusivo de la misma, cesar judicialmente del uso sin autorizacion, la capacidad de exigir la intervencion de las autoridades competentes con el fin de hacer respetar sus derechos, solicitar resarcimiento de daños y perjuicios que se hubieran causado por el uso o empleo indebido, solicitar providencias cautelares previstas en la ley,

denunciar los delitos cometidos en perjuicio de sus derechos y acusar penalmente a los responsable, entre otros.

Delitos contra el patrimonio

El patrimonio se encuentra conformado por los bienes propios o que se adquirieron por cualquier título, pueden ser derechos y obligaciones adquiridos por una persona individual o jurídica. En otras palabras, es lo que le pertenece a la persona y de lo que puede disponer. La Constitución de la República de Guatemala establece distintos tipos de patrimonio como el patrimonio cultura, natural y nacional, lo cual está conformado por un conjunto de bienes y valores descritos que el Estado debe de proteger. Por otra parte, el Código Civil se refiera a distintos tipos de patrimonio, entre ellos, el patrimonio conyugal y familiar. El patrimonio conyugal, se conformará según el régimen económico seleccionado por la pareja al momento de contraer matrimonio. Y el patrimonio familiar estará conformado por los bienes destinados a la protección del hogar. Por lo tanto, se puede decir que el patrimonio es un atributo de la persona, individual o jurídica, y se compone de bienes, derechos y obligación.

El Código Penal guatemalteco, contempla múltiples acciones ilícitas que pueden ser cometidas por las personas en perjuicio del patrimonio. Estas acciones, se encuentran catalogadas según los procedimientos utilizados

por el sujeto activo y contemplan situaciones que agravan el delito. Las categorías establecidas por el cuerpo normativo penal son hurto, robo, usurpaciones, extorsión y chantaje, estafa, la apropiación indebida y defraudación tributaria, los delitos contra el derecho de autor, la propiedad industrial y delitos informáticos, la usura y daños. De acuerdo con De Mata Vela et al (2016), "todos estos delitos, desde el punto de vista de los efectos que se causan en la persona que resiste la acción ilícita, tienen un rasgo común, consiste en el perjuicio patrimonial resentido precisamente por la víctima" (pág. 464). Es decir, los delitos en contra del patrimonio están íntimamente relacionados con el objetivo que el sujeto activo pretende lograr al cometer el ilícito, que es, la afectación de los bienes, derechos y obligaciones del sujeto pasivo o afectado.

Los delitos en contra el patrimonio, se encuentran tipificados en el Decreto número 17-73 emitido por el Congreso de la República de Guatemala, denominado Código Penal, en su del libro segundo título sexto, a partir del artículo 246 al 281. Todos los delitos que se encuentran denominados en este apartado del código están enfocados no solo a proteger la propiedad tangible, sino a la protección jurídica de cualquiera otro derecho que pueda constituir el activo patrimonial de una persona, es decir, todo lo susceptible ser estimado económicamente. Por ejemplo, la distribución de programas destructivos tipificado por el artículo 274 "G", la acción lesiva es causar perjuicio a los registros de computación y en ese caso la

reducción del patrimonio sería los registros mismos y todo lo que el sujeto pasivo deba de invertir para la reconstrucción de dichos archivos y las repercusiones intangibles que está perdida pueda llegar a causarle. El ejemplo está relacionado con la destrucción de la propiedad, pero también está tomando en consideración aquellos aspectos que van más allá de la propiedad misma y tales como los daños y perjuicios que estos le puedan causar y hagan que el patrimonio disminuya.

El Código Penal guatemalteco en el artículo 280 únicamente exime de la responsabilidad penal de los delitos de hurto, robo con fuerza en las cosas, estafa, apropiación indebida y daños. Uno, a los cónyuges o personas unidas de hecho, si estos no han seleccionado la capitulación de bienes separados como régimen económico dentro del matrimonio o la unión de hecho. Dos, a los ascendientes o descendientes consanguíneos o afines. Tres, el cónyuge supérstite sobre las cosas del cónyuge difunto. Y cuatro, entre hermanos, si ellos vivieran juntos. Las causas descritas anteriormente, eximen la responsabilidad penal, pero no eximen de la responsabilidad civil. Por otro lado, el artículo 281 establece como momento consumativo de los delitos de hurto, robo, estafa en el caso de apropiación irregular, cuando el sujeto activo tenga el bien bajo su control.

Delitos contra los derechos de autor, la propiedad industrial y de los delitos informáticos

Las acciones descritas en el Código Penal guatemalteco vulneran el patrimonio de las personas como lo son las obras literarias y artísticas, así como también de todo lo que enmarca la propiedad industrial, ya sean de una persona individual o jurídica. En muchos casos los valores pecuniarios que se le asignan a dichos bienes son subjetivos y cuantificables de acuerdo a varios factores que entre ellos se pueden mencionar, la demanda que estos bienes puedan llegar a tener en cierto momento, el valor que un producto adquiere después de realizar una cantidad de inversión para su desarrollo, el valor que representa una obra literaria o artística y que esto haga que una empresa se coloque en una mejor posición competitivamente en el mercado, la información recabada durante largo tiempo y que tiene como fin la optimización de los recursos y que permita una mejor posición en el momento de establecer precios, entre otros. Cada uno de estos aspectos conllevan importantes montos en investigación y desarrollo que al ser afectados conlleva una disminución en el patrimonio de las personas, por lo que ellas podrían dejar de percibir una cantidad de ingresos esperados o que tiene que volver a invertir cierta cantidad de dinero para recuperar lo que había perdido.

La vulneración de derechos de autor y derechos conexos se encuentra regulado por el artículo 274, el cual describe distintos verbos rectores, las acciones descritas pueden ser realizadas por cualquier persona, ya que no especifica que deba de cumplir alguna característica en específica y el sujeto pasivo está definido, en muchos de los casos, por el titular del derechos aunque en otros es más específico e indica que el sujeto pasivo puede ser específicamente el autor, el productor, el distribuidor legal. Por ejemplo, el inciso a) describe la acción de identificarse falsamente como titular de un derecho de autor. Lo establecido en dicho inciso se refiere en particular a que el sujeto activo presenta como suya una obra literaria o artística, esta acción es comúnmente conocida en el ámbito de la investigación como plagio, el cual no puede ser utilizado con la misma connotación en el derecho penal ya que el plagio esta específicamente enmarcado como delitos en contra de la libertad y la seguridad de la persona. Y así describe 22 incisos, que describen acciones que vulnera el derecho de autor. Todas las acciones descritas por el artículo 274 tienen pena de prisión de uno a seis años y multa de cincuenta mil a cien mil quetzales.

El último párrafo de artículo 274 establece “los supuestos contenidos en esta disposición se determinarán con base en las disposiciones aplicables de la Ley de Derecho de Autor y Derechos Conexos” (Código Penal, 1973). Dentro de las disposiciones aplicables se regulan, en el caso que

sea necesario hacer valer derechos reconocidos por el Decreto número 33-98 deberán de hacerse ver por la vía civil en juicio oral o métodos alternativos como la conciliación y el arbitraje. Tomando en consideración que el principio de intervención mínima impide en un Estado democrático la expansión del derecho penal, debiendo quedar este reducido a su mínima expresión. (González Cauhapé-Cazaux, 2009, pág. 19), es decir que de existir una controversia el sujeto pasivo debe realizar una acción civil o mercantil ya que la intervención penal no es necesaria y esta debe de ser necesaria.

El delito que afecta la propiedad industrial se encuentra regulado en el artículo 275 del Código Penal, el cual se refiere a la violación de los derechos de propiedad industrial. Así como el artículo 274, este también cuenta con la descripción de verbos rectores que indican la acción que el sujeto activo debe de cometer para violentar el patrimonio del sujeto activo. De ser cometido este delito se podrá tener una pena de prisión de uno a seis años y multa de cincuenta mil a setecientos cincuenta mil quetzales. De igual forma este delito también se atiene a las disposiciones establecidas en su ley específica, el Decreto número 57-2000 y como indica De Mata Vela et al. (2016) "podrían ser sancionados en leyes administrativas, atenta contra el principio doctrinario de mínima intervención del Derecho Penal, siendo preferible en este" (pág. 503).

El Código Penal guatemalteco al referirse a los delitos informáticos, los cuales surgen como respuesta a lo vulnerable que se encuentra la información por los avances tecnológicos en las computadoras, su incremento en la cantidad de procesamiento y almacenamiento, también debido a la facilidad que el internet y las telecomunicaciones brindan para acceder a ella. Este tipo de delitos pone en riesgo el patrimonio digital de las personas, el cual es similar al derecho de autor y propiedad industrial, ya que actualmente esto abre puertas a un abanico de posibilidades y escenarios que perjudiquen la propiedad digital de las personas. Guatemala actualmente tipifica los delitos informáticos dentro del Código Penal, que comprenden desde el artículo 274 "A" al 274 "H", los cuales fueron incluido por las reformas realizadas en el año 1996 por el Decreto 33-96 del Congreso de la República de Guatemala, como parte del conjunto de reformas que pretendían actualizar el Decreto número 17-73.

El artículo 274 "A" describe que comete el delito de destrucción de registros quien destruya, borre o de cualquier modo inutilice, altere o dañe registros informáticos. Será sancionado con prisión de seis meses a cuatro años y multa de dos mil a diez mil quetzales y si tuviera el propósito de obstaculizar una investigación o procesamiento de carácter penal será sancionado con prisión de tres a seis años e inhabilitación especial. De esta forma se entiende que los registros informáticos, es un secreto empresarial por ser información no divulgada y la cual es utilizada en un tipo de

actividad productiva, industrial, comercial o de servicios y si puede ser susceptible de transmitirse a un tercer con el adecuado acuerdo de confidencialidad. Este delito contempla un agravante al ser esta información ser parte en un proceso y su destrucción obstaculice el mismo.

Para entender el artículo 274 “B” que se refiere al delito de alteración de programa, es importante tener claro que está haciendo referencia a un programa de computadora, el cual se define como una secuencia de instrucciones lógicas que tiene como objetivo el procesamiento de la información con un fin específico. Es decir, quien altere, borre o inutilizare las instrucciones o el programa en general y que dichas acciones no permitan que este cumpla con su fin, será sancionado con la misma pena que el delito de destrucción de registros informáticos, con pena de prisión de seis meses a cuatro años y multa de dos mil a diez mil quetzales. Y en caso acción realizada por el sujeto activo estuviere destinada a obstaculizar una investigación, será sancionado con prisión de tres a seis años e inhabilitación especial.

La reproducción de instrucciones o programas de computación tipificado por el artículo 274 “C”, es un claro ejemplo de la distinción entre delitos y ciberdelito. Como se indicó anteriormente, los ciberdelitos surgen de las acciones que no fueran posibles de no existir el internet y las tecnologías de la información y comunicación, es evidente que este delito es similar

al descrito en el artículo 274 literal c) del Código Penal. Ambos indican que, de reproducirse la propiedad del sujeto activo, en un caso una obra y en el otro un programa de computación, sin autorización del autor será sancionado. La sanción es más grave para el delito que vulnera los derechos de autor, ya que esta seria de uno a seis años y multa de cincuenta mil a setecientos cincuenta mil quetzales, en cambio en el delito informático la sanción será de prisión de seis meses a cuatro años y multa de quinientos a dos mil quinientos quetzales. Es posible que el legislador le dio su lugar a la piratería de *software*, aunque tal vez en ese momento no se dio cuenta de las cantidades de dinero que genera el licenciamiento de los programas de computación a los desarrolladores. Hoy en día los desarrolladores han cambiado los modelos de licenciamiento de sus aplicaciones, para minimizar la cantidad de pérdidas que tenían. Pero esto ha cobrado una gran factura a las empresas que desaparecieron por no contar con la certeza jurídica que protegiera su patrimonio.

Los registros prohibidos descrito por el artículo 274 “D”, se refiere a la creación de bancos de datos o registros informáticos que pueda afectar la intimidad de las personas. Y serán sancionados con prisión de seis meses a cuatro años y multa de doscientos a mil quetzales. La manipulación de información se da por utilizar registros informáticos o programas de computación para ocultar, alterar o distorsionar información requerida para una actividad comercial, para el cumplimiento de una obligación

respecto al Estado o para ocultar, falsear o alterar los estados contables o la situación patrimonial de una persona física o jurídica y será sancionado con prisión de uno a cinco años y multa de quinientos a tres mil quetzales. El delito de uso de información es cometido por quien, sin autorización, utilice u obtenga para sí o para otro, datos contenidos en registros informáticos, bancos de datos o archivos electrónicos. Se le impondrá la pena de prisión de seis meses a dos años y multa de dos mil a diez mil quetzales. Todos los delitos descritos anteriores se basan en el propósito, la obtención y el tratamiento que se le dé a la información.

El artículo 274 "G" describe el delito de programas destructivos es cometido por quien distribuya o pusiere en circulación programas o instrucción destructivas, que puedan causar perjuicios a los registros, programas o equipos de computación y serán sancionados con prisión de seis meses a cuatro años y multa de doscientes a mil quetzales. Este delito es conocido comúnmente para los que crean los virus de computadora, que hoy en día siguen surgiendo una gran cantidad de ataques, pero no necesariamente pueden ser ejecutados desde la misma ubicación y esto genera una complejidad al momento de la persecución penal ya que no solo pueden ser ejecutados desde otras partes del mundo, sino que ahora existen una mayor cantidad de métodos que causen perjuicios a los registros, programas o equipos de computación. Por lo tanto, la comunidad

internacional está generando alianzas internacionales para la cooperación entre Estados que permitan la persecución penal de los ciberdelitos.

El delito de alteración maliciosa de números de origen tipificado por el artículo 274 “H”, es cometido por quien valiéndose de cualquier mecanismo altere el número proveniente de un operador extranjero de telefonía utilizando exclusivamente para tráfico internacional, o altere el número de identificación del usuario de origen una llamada de telefonía será sancionado con pena de prisión de seis a diez años. De Mata Vela hace ver que existe un defecto en la redacción, ya que el acápite establece la alteración maliciosa, pero la palabra maliciosa no se encuentra establecida en el verbo rector y esto hace que cualquier tipo de alteración ya es susceptible de ser perseguido penalmente, sea o no maliciosa. Adicionalmente hace referencia que dicho operador de telefonía debe de ser exclusivamente extranjero (Derecho penal guatemalteco tomo II parte especial, 2016, pág. 208).

El delito descrito en el párrafo anterior, hasta cierto punto sigue siendo vigente pero no positivos del todo. Debido a que hoy en día la forma en que nos comunicamos va más allá de utilizar operadores telefónicos, gracias a los avances tecnológicos han surgido proveedores de aplicaciones como la mensajería instantánea, entre ellos *whatsapp* o *telegram*. Quienes utilizan el termino de voz sobre de *ip*, denominada

VoIP por sus siglas en inglés *voice over ip*, el cual hace referencia a que transforman la voz de una señal analógicas a una combinación de unos y ceros, es decir una señal digital, y permiten realizar llamadas sin utilizar a los operadores de telefonía, locales o extranjeros. En este caso, los administradores de los sistemas de mensajería instantánea, en vez de asociar un número telefónico a la persona, la asocian a una cuenta de correo o un usuario registrado en su plataforma, el cual permanece con la persona indistintamente del dispositivo que esté utilizando.

Los sistemas de mensajería instantánea indicados en el párrafo anterior, también utilizan métodos secundarios asociados a los dispositivos telefónicos como la identificación de direcciones de protocolo de internet denominada direcciones *ip* por sus siglas en inglés *internet protocole address*, quienes está compuesta por cuatro pares de dígitos hexadecimal, los cuales no son controlados por operadores telefónicos sino por *proveedores de servicio de internet* comúnmente conocidos como *ISP* por sus siglas en inglés *internet service provider*. Todo esto con el fin de ejemplificar los tecnicismos y la complejidad que surgen por los avances tecnológicos y como afectan esto la redacción y la desactualización de las normas vigentes.

La suplantación de identidad en el Derecho Comparado

La suplantación de identidad digital

La etimología de la palabra, suplantación de identidad digital, surge a raíz de la unión de dos conceptos. El primer concepto es la suplantación, definida por Real Academia Española como "Ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba", en otras palabras, es tomar el lugar de alguien valiéndose de engaños vulnerando el derecho de esta persona a quien se suplanto. El segundo concepto, la identidad digital, es el conjunto de características que lo hacen único diferenciándola de otros en el ciberespacio. Es decir, la suplantación de identidad digital es cuando una persona denominada sujeto activo, toma las características digitales que identifican a otra persona denominada sujeto pasivo, valiéndose de medios poco éticos, para vulnerar el derecho de este o de un tercero.

La comisión de suplantación de identidad digital a lo largo del tiempo ha evolucionado por la cantidad de usuarios que tienen acceso al ciberespacio, también debido a los distintos tipos de servicios a los cuales estos usuarios tienen acceso. Hoy en día encuentran servicios como, las redes sociales, las cuales son plataformas estructuradas para que las personas interactúen desde sus casas u oficinas de trabajo con otras personas que tengan los mismos intereses. Existen distintos tipos de redes

sociales, unas enfocadas en ocio, otras para tener presencia como empresa y realizar contrataciones de personal o difusión de información empresarial, también se encuentran espacios en donde se pueden difundir ideas y que otras personas comenten con el objetivo del intercambio de opiniones, existen redes sociales para el intercambio de arte y actualmente están muy frecuentadas redes en donde se pueden realizar transacciones de monedas digitales. Para interactuar en estas redes sociales, las personas deben de identificarse con las características mínimas un nombre único, correo electrónico y una foto de perfil. La identificación dependerá de los niveles de seguridad implementados por cada uno de los proveedores de servicios.

Otro de los servicios más utilizados por las personas ya sean individuales o jurídicas en el ciberespacio es el correo electrónico, el cual es un servicio de correo en donde se comparte información electrónica con destinatarios y en muchos de los casos las empresas o las personas lo utilizan para la difusión de información catalogada como información sensible y/o personal, también es muy comúnmente utilizado para realizar confirmaciones de seguridad. El correo electrónico generalmente es de uso gratuito, por lo cual permite que muchos más usuarios utilicen esta herramienta, también está la opción de utilizar el servicio por membresía el cual conlleva de un pago mensual o anual, el cual brinda características adicionales a los gratuitos, como el uso de nombres de domino

personalizados que identifican a una organización en específico. El correo electrónico es una herramienta la cual se ha convertido en básica para realizar cualquier transacción y en la mayor de los casos es utilizada de forma correcta pero también es utilizada para confundir a las personas y que esta proporcione información que permita vulnerar la seguridad y por ende vulnerar algún bien jurídico tutelado por los Derechos Humanos.

Por otro lado, los sitios en internet son también servicios que requieren de proveedores de servicios en el ciberespacio y que son una representación virtual de las empresas. En este caso las empresas pagan por contar con un espacio público o privado y mostrar su información para que puedan ser contactados por clientes o por cualquier persona que requiera contactarlos, hoy en día esto ha sido una necesidad para las personas y que tengan presencia en el ciberespacio. A través de los sitios en internet, por ejemplo, los bancos establecen portales en donde los usuarios se deben de autenticar ingresando sus credenciales y una vez autenticados podrán realizar un abanico de operaciones sin tener que presentarse en una agencia física.

También de igual forma hoy en día con el auge de las cripto monedas distintos proveedores financieros ponen a su disposición sitios internet en donde prestan sus servicios y los usuarios de igual forma que las instituciones bancarias deben de autenticarse y una vez hecho esto, podrán realizar transacciones de monedas electrónicas. Igualmente existen sitios

en internet en donde se pueden comprar bienes o servicios y las personas individuales o jurídicas con el objetivo de realizar una compra deben de ingresar la información de sus tarjetas de crédito para concretar la compra.

Como se describió anteriormente existen servicios que hoy por hoy son fundamentales para la convivencia, el intercambio de información y para el comercio. Cada uno de estos servicios son susceptibles a ser suplantados digitalmente con propósitos de dañar a una persona en especial o de utilizarlo como medio para cometer otro ilícito. Y existen muchos métodos los cuales surgen según las posibilidades que el ciberespacio provee, en donde los ciberdelincuentes realizan ingeniería social valiéndose de métodos como la suplantación de identidad digital para engañar a las personas y por medio de este engaño, estas personas proporcionen sus credenciales y esto les permita realizar transacción en nombre de otra persona. También hay que verlos desde el punto de vista en donde la suplantación de identidad digital, los ciberdelincuentes toman los signos distintivos de las empresas, las imágenes de la marca, nombres comerciales, imágenes de emblemas, entre otros para estructurar sitios en internet, correos electrónicos y perfiles de redes sociales en donde engañan a terceros, desprestigiando a las instituciones o personas quienes invierten tiempo y dinero en la creación de la propiedad industrial, y que al final de cuentas representa en pérdidas por desacreditación de la imagen pública que cada una de las personas pueda tener en el ciberespacio.

El Convenio de Ciberdelincuencia de Budapest

El Consejo de Europa es una organización internacional formada por 47 miembros en los cuales se incluyen 28 Estados miembros de la Unión Europea. En donde los Estados cooperan para la creación de espacios políticos y jurídicos, basados en democracia, derechos humanos y el imperio de la ley. Con el fin de desarrollar principios democráticos comunes entre sus miembros para favorecer el progreso económico y social. El Consejo de Europa fue fundado en 1949 y tiene su sede en Estrasburgo, Francia. Se conforma por dos órganos, la Asamblea Parlamentaria y el Comité de ministros. La Asamblea Parlamentaria está compuesta por los representantes de los parlamentos nacionales de los 47 Estados miembros y el Comité de ministros, está conformado por los ministros de Asuntos Exteriores de los Estados miembros y este es el órgano que toma las decisiones en el Consejo de Europa.

El convenio de ciberdelincuencia de Budapest fue desarrollado por el Consejo de Europa y los Estados signatarios y aprobado por el comité de ministros del Consejo de Europa en la 109 reunión, llevada a cabo el 23 de noviembre de 2001 en Budapest, Hungría. Estableciendo como objetivo, la creación de una política penal con el objeto de proteger a la sociedad frente a la ciberdelincuencia. Proponiendo la adopción de cooperación internacional y una legislación estándar, que se adapte a los

cambios que enfrentan las personas por la digitalización, la convergencia y la globalización continua del internet, las tecnológicas de la información y de la comunicación. El consejo de Europa preocupado por lo vulnerable de las personas frente a los riegos generados al utilizar el ciberespacio y hacerlo parte de su vida cotidiana, ya que este es utilizado como una herramienta de trabajo y de comercio, en donde se realizan transacciones de toda índole, susceptibles a delitos.

El Consejo de Europa y los Estados signatarios, consideran que con el fin de hacerle frente a la lucha en contra de la ciberdelincuencia es necesaria una cooperación internacional en materia penal. Hay que tomar en cuenta que el Convenio de Ciberdelincuencia es necesario para evitar poner en peligro los datos, los sistemas, la integridad de la información, la confidencialidad, los bienes digitales, las obras artísticas, las marcas distintivas, los emblemas, las invenciones, la seguridad, garantizando la tipificación como delitos dichos actos que vulneren los derechos de la propiedad de las personas. Y con el presente convenio pretenden proveer a los Estados signatarios de herramientas para luchar en contra de los delitos que puedan surgir a raíz de los avances tecnológicos. Estas herramientas facilitaran la investigación y sanciones, ya sea por delitos cometidos en el mismo territorio o extranjero, con normas jurídicas que permitan la cooperación internacional.

El Convenio de Ciberdelincuencia de Budapest toma en consideración distintos convenios para mantener un equilibrio entre los intereses del derecho penal y el adecuado resguardo de los derechos fundamentales, derechos establecidos en tratados internacionales, derechos que protegen los datos personales, los derechos de los niños, entre otros. Entre los cuales se pueden mencionar, el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1996), el Convenio de 1981 del Consejo de Europa para la protección de las personas con respecto al tratamiento informatizado de datos personales, la convención sobre los Derechos del Niño de las Naciones Unidas (1989) y el Convenio sobre las peores formas de trabajo infantil de la Organización Internacional del Trabajo (1999).

Adicionalmente a los tratados internacionales, el Convenio de Ciberdelincuencia de Budapest, toma en consideración las siguientes prácticas, la vigilancia de las telecomunicaciones, medidas en contra de la piratería en materia de propiedad intelectual y derechos afines, buenas prácticas referentes a la protección de datos personales en el ámbito de los servicios de telecomunicaciones, la delincuencia relacionada con la informática. Todo esto con el fin de proporcionar plantillas que apoyen a los legisladores para establecer leyes en donde establezcan ciberdelitos y procedimientos penales vinculados a la tecnología de la información, como los medios de investigación eficaces en materia de delitos

informáticos y mecanismos rápidos y eficientes de cooperación internacional en contra de los ciberdelincuentes.

El convenio dispone de cuatro capítulos entre los cuales se encuentran, la terminología a utilizar dentro del documentos, las medidas que deberían ser adoptadas dentro del ordenamiento jurídico, tanto sustantivo como procesal, también establece los protocolos de cooperación internacional y clausulas finales. Dentro del capítulo II en donde se discute temas referentes a las disposiciones relativas a los delitos en el ámbito informático o los delitos relacionados con el uso de computadores, se definen nueve delitos segmentados en cuatro categorías. Los delitos definidos son, acceso ilícito, interceptación ilícita, ataques a la integridad de los datos, ataques a la integridad del sistema, abuso de dispositivos, falsificación informática, fraude informático, delitos relacionados con la pornografía infantil y delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.

Adicionalmente el capítulo II abarca el ámbito procesal, la cual se divide en dos secciones. La primera está enfocada en establecer las siguientes actividades, el resguardo efectivo de los datos almacenados, resguardo y publicación parcial de los datos relacionados al tráfico, el orden de presentación dentro del proceso, el registro y la confiscación de los datos almacenados, la obtención é interceptación en tiempo real de datos

asociados al delito. En la segunda sección establece parámetros referentes a la jurisdicción. El capítulo III establece las disposiciones relacionadas a la colaboración de los delitos convencionales y los ciberdelitos, entre las disposiciones establecidas se encuentra los términos de la extradición. Al referirse a la colaboración respecto a los ciberdelitos, establece un tipo específico de acceso transfronterizo a los datos y recomiendo la utilización de una red que funcione 24 hora los 7 días de la semana con el fin de asegurar la asistencia rápida entra las partes. Y por último el capítulo IV establece disposiciones finales.

Como parte introductoria del Convenio de Ciberdelincuencia de Budapest, el artículo 1 abarca definiciones importantes de temas que serán tratados dentro del presente convenio. El inciso a. define sistema informático, en donde hace referencia que este puede ser tanto un componente físico como lógico de una computadora, la cual tiene puertos o también denominados periféricos, con los cuales el usuario puede interactuar conectando accesorios externos y son utilizados por ejemplo para la conexión de dispositivos de almacenamiento externos. Establece que los sistemas informáticos tienen la posibilidad de funcionar de forma independiente, es decir aislados de cualquier comunicación externa, o estar interconectados por medio de redes de comunicación a otros dispositivos con los cuales interactúan los seres humanos, entre ellos otros sistemas informáticos y puede estar limitada geográficamente a pequeñas áreas llamadas LAN por

sus sigla en inglés *local area network* o a áreas extensas denominadas WAN por sus siglas en inglés *wide area network*. Una combinación de ambas es el internet, la cual es capaz de compartir información con otros sistemas informáticos.

El sistema informático, tiene la capacidad de actuar por si solos, es decir de forma automática, sin intervención de un usuario. Esto es posible a que ejecutan instrucciones dadas por programas informáticos que son ejecutados para lograr un objetivo específico que es el tratamiento de los datos, en otras palabras, el usuario provee de cierta información que es considerada como la información de entrada y el programa al detectar que cuenta con nueva información, ejecuta las instrucciones con el fin de procesar dicha información transformándola en información resultante denominada información de salida. Esta información ya procesada es utilizada por el usuario o por quien corresponda, es decir puede ser también utilizada por otros sistemas de información, para un fin determinado. Entre ellos, podríamos mencionar como ejemplo, la estrategia de mercadeo de una multinacional, el cálculo del pago de prestaciones de los empleados de cierta empresa, los diseños secretos de un sistema patentado el cual genera ventajas competitivas al momento de la determinación de los costos en cierto producto, entre otros.

El inciso b. del artículo uno establece que se entenderá por datos informáticos todo lo que se preste a tratamiento informático, esto quiere decir, que la información se encuentra en un formato que pueda ser procesado por un sistema informático. De esa forma se entenderá que el termino dato, hace referencia a que tiene un formato electrónico o una cuenta con una estructura definida que permita ser manipulado por un programa de instrucciones. Por ejemplo, se puede mencionar un documento o un archivo que sería nuestra información de entrada y el objetivo será tener la capacidad de abrir ese archivo y que pueda ser manipulado por un procesador de palabras, hoy en día es común utilizar *Microsoft Word*® el cual tiene múltiples extensiones de archivo, según el objetivo del usuario, pero principalmente se utilizan las extensión de archivos .docx o .doc, esto quiere decir que el archivo o datos informáticos que estén guardados con esta extensión pueden ser manipulados por este procesador de palabras y producir un resultado que sería el documento ya procesado. Estos datos de información según el presente convenio están sujetos a medidas de investigación según el caso y el momento procesal oportuno.

Continuando con las definiciones establecidas con el artículo uno, el inciso c. define el termino proveedor de servicio, quienes en el ciberespacio existen una gran variedad quienes juegan un papel muy importante referentes a las comunicaciones y el tratamiento de los datos a

través de sistemas informáticos. Existen dos categorías fundamentales, la primera es la que permiten la comunicación entre sistemas informáticos, quienes pueden ser entidades publica o privadas. En este caso son entidades que proporcionan servicios de internet. Por otro lado, la segunda categoría a la que hace referencia son los proveedores que procesan o almacenan datos informáticos, en este caso hoy en día los sistemas financieros proveen sus servicios a través de plataformas o sistemas de información publicados en el internet, en donde el usuario tiene la posibilidad de realizar transacciones. De igual forma funciona el correo electrónico tiene la posibilidad de ser proveído por prestadores de servicios en donde se envía datos informáticos a través de ellos.

Por último, el incido d. el cual define los datos relativos al tráfico, en este caso determina que estos datos son los utilizados para realizar la comunicación en sí, desde un punto de vista técnico, estos datos son los que encapsulan los datos informáticos y contienen la información del origen y el destino de hacia dónde deben de ser dirigidos. Esta información es relevante para las investigaciones ya que permiten determinar el origen de la comunicación y reunir las pruebas que fundamente una hipótesis planteada por un investigador en un proceso penal. Esta información debido a su volatilidad debe de ser tratados rápidamente con el fin de conservar la integridad. Las características principales de los datos relativos al tráfico son, el origen, el destino, la ruta, la hora, la fecha, el

tamaño y la duración de la comunicación o el tipo de servicio subyacente. En el caso del origen y el destino, es decir, las direcciones lógicas del equipo que está enviando la información y del que la recibe. Respecto a la ruta, se refiere a las direcciones lógicas de los enrutadores por los que transito la información. Al referirse al tipo de servicio subyacente, hace referencia al tipo de sistema de información o proceso que manipula la información. Por ejemplo, en el caso del sistema de información como el correo electrónico, el cual es puesto al servicio por un proveedor en específico o en el caso de procesos generados por aplicaciones, los cuales ejecutan tareas que manipulan la información.

El capítulo II, denominado medidas que deberán adoptarse a nivel nacional, se encuentra dividido en tres secciones. La sección número uno abarca lo referente al derecho penal sustantivo y este se encuentra divido en cinco títulos. Esta sección, abarca del artículo 2 al 13, los cuales son representan el resultado de un consenso, de los delitos que como mínimos de deben de tomar en consideración en común por los Estados, pero no excluye los delitos que puedan adoptarse individualmente por cada uno de ellos, ya que esto facilitara la lucha y colaboración entre ellos para confrontar dichas acciones ilícitas en el ámbito nacional e internacional. Ya que, de existir parámetros en común entre las leyes de cada uno de los países, se puede evitar que los sujetos que cometieron el delito trasladen sus casos a jurisdicciones que cuenten con penas menores o que no

contemple estos tipos ilícitos. Otro de los beneficios de estandarizar las acciones ilícitas es que al momento de requerir la cooperación internacional y sea necesaria la extradición, esta se va a ver facilitada por ejemplo en los requisitos de doble tipificación penal.

El titulo primero incluye los delitos principales, los cuales van del artículo dos al seis, descritos a continuación. En el artículo dos, el acceso ilícito, a un sistema informático infringiendo medidas de seguridad con el objetivo de obtener datos informáticos o cualquier otra intención ilegitima; por otra parte el artículo tres, la interceptación ilícita, de una transmisión privada dentro de un mismo sistema u originada desde uno de ellos o entre distintos sistemas, valiéndose de cualquier medio o tecnología; En el artículo cuatro, ataques a la integridad de los datos, y en este caso hay que tomar dos consideraciones, la primera es que es un acto ilícito que dañe, borre deteriore, altere o suprima datos informáticos y la segunda consideración es que se deben de tomar en cuenta agravantes que generen daños más graves.

Continuando con el título primero, en el artículo cinco, ataques a la integridad de sistemas, es la obstaculización ilícita del funcionamiento de un sistema informático, valiéndose de cualquier medio que no permita la adecuada ejecución de sus funciones; En el artículo seis, abuso de los dispositivos, este es un delito que surge de la venta, reproducción o

cualquier otra forma de reproducción de las claves, códigos de accesos o datos informáticos y dispositivos que permitan acceder a un sistema de informático con intención de que sea utilizado para cometer los delitos establecidos en los artículos del dos al cinco de este convenio y la posesión de alguno de esos elementos, permitirá la exigencia de la responsabilidad penal.

Posteriormente el convenio establece el titulo segundo, en donde fueron agregados artículos por recomendación del Consejo de Europa y se concentra en dos delitos. El primero el artículo siete, falsificación informática, el cual tipifica la acción de introducir, alterar, eliminar o eliminar deliberada e ilegítimamente los datos informáticos que genere datos no auténticos con la intención de que sean considerados como auténticos para efectos legales; Y el artículo ocho, fraude informático, como la introducción, alteración o eliminación de datos informáticos o también, por la manipulación en el funcionamiento que afecte a un sistema informático con intención de obtener de forma ilícita un beneficio económico.

A continuación, el titulo tercero, describe el contenido de los delitos de la producción o distribución ilícita de pornografía infantil mediante el uso de sistemas informáticos. El cual abarca el artículo nueve, delitos relacionados con la pornografía infantil, establece que cada uno de los

Estados adheridos al convenio deben de adoptar medidas legislativas y de cualquier otro tipo para sancionar, la producción, la puesta a disposición, la difusión o adquisición y la posesión de pornografía infantil. También define que se considerara, pornografía infantil, todo aquel material pornográfico que contenga la representación visual de un menor o quien parezca menor, adoptando un comportamiento sexual explícito. Y se considerara menor a toda persona menor de 18 años, pero deja a discreción del legislador que la edad mínima inclusive puede ser de 16 años.

En el titulo cuarto, establece los delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines. Y estos son los delitos en donde más se utiliza el internet y las tecnologías de la información y comunicación para su comisión. El cual básicamente se concentra en el artículo diez, el cual establece que cada uno de los Estados adoptara las regulaciones que protejan los derechos de los compromisos contraídos por los convenios firmados con distintas organizaciones. Como, las obligaciones contraídas con el Convenio de Berna para la protección de las obras literarias y artísticas, el Acta de Paris de 1971, el Acuerdo sobre los Aspectos de los Derechos de Propiedad Intelectual relacionados con el Comercio, ADPIC y el tratado de la Organización Mundial de Propiedad Intelectual, OMPI. Ambos denominados así por sus siglas en español.

Y por último el titulo quinto, el cual, cubre temas como la tentativa, la complicidad, así como la penas y los instrumentos internacionales y responsabilidades de las personas jurídicas. El Convenio de Budapest en su artículo once deja a libertad de las partes adherentes la potestad de regular la complicidad, que se pudiera llegar a tener en los actos ilícitos cometidos en desde artículo dos al artículo diez y la tentativa en las acciones ilícitas cometidas por los delitos previstos del artículo tres al cinco, así como del artículo siete al artículo ocho e incluyendo el artículo nueve numeral uno inciso a e inciso c. El convenio delega en las partes el derecho de aplicar o no las sanciones a los actos calificados como tentativa, como lo expresa en el tercer párrafo del artículo once.

El artículo doce recomienda a las partes regular las medidas que sean necesarias para que los damnificados tengan las herramientas que les permitan exigir responsabilidad penal a las personas jurídicas por los delitos previstos por el Convenio ciberdelincuencia de Budapest, cuando estos sean cometidos por personas físicas a título individual o en representación de la persona jurídica. También establece que cada parte debe de adoptar o tomar en consideración dentro de sus cuerpos normativos, exigir la responsabilidad a las personas jurídicas que no vigilen o monitoreen a las personas físicas que los representan y que este actúe por cuenta propia sin autoridad de la persona jurídica. Y por último el artículo trece establece que queda a discreción de cada parte establecer

las penas y sanciones que sean efectiva y disuasorias a la persona jurídica, con el fin de evitar la comisión de los delitos establecidos del artículo dos al artículo once de este convenio.

La sección número dos, la cual está enfocada en el derecho procesal, abarca del artículo catorce al artículo veintitrés y se encuentra dividido en cinco títulos. El titulo primero regula que cada parte adoptara el ámbito de aplicación de las disposiciones de procedimientos a efecto de investigación o de procedimientos específicos y queda en cada uno de los países contratantes adoptar las medidas legislativas para establecer poderes y procedimientos. El titulo segundo, referente a la conservación rápida de los datos informáticos almacenados, es decir, lo datos que ya se encuentran almacenados deben de ser protegidos con el objetivo de evitar deterioro o modificaciones y en el peor de los casos evitar que sean eliminados. Esto también aplica para la transmisión de datos, en donde se deben de involucrar a los proveedores de servicios a que apoyen a las autoridades para resguardar y apoyar a las autoridades cuando así sean requeridos.

En el titulo tercero, la orden de presentación es en resumen la facultad la cual tendrá el órgano jurisdiccional de solicitar a las personas o proveedores de servicios la presentación de la información almacenada o los datos referentes al tráfico de las transmisiones de los datos. En el titulo

cuarto, registro y confiscación de datos informáticos almacenados, es dotar de herramientas a las autoridades, que les permitan obtener pruebas relacionadas con una investigación en específico y que vaya de la mano con los procedimientos penales. Por último, en el titulo quinto, la obtención en tiempo real de datos informáticos en donde se establece que cada parte contratante del convenio debe de adoptar las medidas legislativas que faculten a las autoridades competentes a resguardar en tiempo real o interceptar los datos o el tráfico.

Para finalizar la sección número tres del capítulo II la cual, describe los aspectos a considerar en la jurisdicción. Basado en el principio de territorialidad, cada parte se compromete en adoptar las penas que sancionen los delitos descritos en el presente convenio y que sean cometidos en el territorio. De igual forma se deben de considerar las sanciones a las personas o proveedores de servicios que no colaboren con los procedimientos establecidos para la obtención de las pruebas y quienes alteren o eliminen la información confiscada. El capítulo III, que trata la cooperación internacional y se encuentra dividido en dos secciones. La sección primera, establece los principios rectores de la cooperación internacional, entre ellos el principio de extradición y asistencia mutua. Y la sección segunda, que ya son disposiciones específicas como la asistencia mutua en materia de medidas provisionales y con los poderes de investigación. Lo cual lleva a una red de 24/7, es decir un punto de

contacto el cual se pueda contactar las veinticuatro horas, los siete días de la semana, con el fin de garantizar una asistencia inmediata para la investigación relativa a los delitos.

En el capítulo cuarto, referente a las cláusulas finales, entre los puntos más importantes establece la adhesión al convenio, en donde previa consulta con los Estados contratantes del convenio y habiendo obtenido su consentimiento unánime, podrán invitar a adherirse a cualquier Estado que no sea miembro del Consejo de Europa. El Ministerio de Gobernación de la República de Guatemala, reporto el día 24 de abril de 2020 que el Comité de ministros del Concilio de Europa aprobó la solicitud de Guatemala de acceder a la Convención de Budapest. En donde a partir de esta fecha se han presentado múltiples iniciativas de ley que adopten las disposiciones del presente convenio y recientemente fue emitido por el Congreso de la República de Guatemala el Decreto 11-2022, el cual incluye nuevos delitos que sancionan hechos cometidos valiéndose de medios tecnológicos y que pretenden proteger a la niñez y adolescencia, contra la seducción por medios digitales, engañan o amenazan a menores de edad para que envíen material de contenido sexual.

En el Convenio de Ciberdelincuencia de Budapest, no se encuentra explícitamente regulado el delito de suplantación de identidad digital. Pero como se describió anteriormente en el artículo diez del presente convenio,

cada una de las partes podrá adoptar otros delitos dentro del derecho interno de conformidad con acuerdos contraídos que protejan el derecho de autor y el de propiedad intelectual.

Ley número 146 de 30 de julio de 2012 Código Penal de Puerto Rico

A pesar de que Puerto Rico es un país ubicado geográficamente en el Caribe, es un Estado asociado a Estados Unidos de Norte América, con un territorio de 9,104 kilómetros cuadrados, una población total de 3,194,034, un producto interno bruto de 103,14 mil millones de US$ y el 78% de la población usan internet, datos reportados en el 2019 por el Banco Mundial. Que desde un punto de vista económico son valores por debajo de la media de los países latinoamericanos. Pero una de las ventajas con las que cuenta es que, por ser una Estado asociado a los Estados Unidos de Norte América, comparte mucho de los principios de un país de economías subdesarrolladas en comparación a la económica guatemalteca o a la media de los países centroamericanos. Entre las buenas prácticas que Puerto Rica a acuñado es la tipificación del delito de suplantación de identidad digital, y esto se debe a que los Estados Unidos de Norte América cuenta con estándares muy elevados al momento de legislar las amenazas cibernéticas ya que es uno de los países con mayor cantidad de ataques realizadas por ciberdelincuentes.

De acuerdo con el IC3 denominado por sus siglas en inglés *Internet Crime Compliant Center*, cual es un departamento del Buró Federal de Investigación FBI denominado de igual forma por sus siglas en inglés *Federal Bureau of Investigation*, que significa Buró Federal de Investigación y es el principal ente investigador del departamento de justicia de los Estados Unido de Norte América, en su reporte *Internet Crime Report del 2021* mostro que la cantidad de víctimas por ciberdelitos en Puerto Rico fue de 1,923 y se calcula que represento perdidas de US$14,650,062. En donde el robo de identidad se encuentra entre los principales delitos cometidos estimados por el IC3, haciendo una especial connotación a que el año 2021 es uno de los años atípicos por causa de la pandemia vivida a nivel mundial denominada COVID-19, que dio apertura a mayor cantidad de modelos de comercialización a través de redes sociales, apoyándose más del correo electrónico personal y creando mayor cantidad de sitios en internet.

El ordenamiento jurídico penal puertorriqueño en el Código Penal, Ley 146-2012, en su artículo 209 Apropiación ilegal de identidad establece "Toda persona que se apropie de un medio de identificación de otra persona con el propósito de realizar cualquier acto ilegal, será sancionado con pena de reclusión por un término fijo de ocho años" el artículo en su tercer párrafo es muy explícito al determinar cuáles son los medios de identificación que son susceptibles de apropiación ilegal entre los cuales

se encontraran el correo electrónico, un sistema de computadoras o cualquier otro dato que pueda ser utilizado por si o junto con otros para identificar a una persona. Y en su último párrafo establece que se tendrá como agravante cuando haya cometido en la realización de transacciones comerciales o de cualquier otra índole que afecte derechos individuales o patrimoniales de la víctima.

La apropiación ilegal de identidad al no establecer en su acápite el termino digital, no quiere decir que no tome en consideración los ciberdelitos. Ya que como se vio anteriormente establece explícitamente ciertas características o servicios que surgen a la vida por el internet, las tecnologías de la información y la comunicación, como lo son el correo electrónico y los sistemas de computadoras. Eso sí, sin establecer algún agravante alguno por el mero hecho de ser un ciberdelito o delito informático, sino los agravantes que establece están dados por haber realizado transacciones o afectar derechos patrimoniales. Que entre los derechos patrimoniales que pueden ser vulnerados entre ellos se encuentra la propiedad industrial, así como los derechos de autor.

Ley número 53-07 sobre crímenes y delitos de alta tecnología de la República Dominicana

La República Dominicana es un país de igual forma que Puerto Rico, se encuentra ubicado en la región del Caribe y cuanta con un territorio de 48,442 kilómetros cuadrados, una población total de 10,847,904 y un producto interno bruto de 78.84 mil millones US$, el 77% de las personas usan internet, según los datos reportados por el Banco Mundial en el año 2020. La República Dominicana y Costa Rica al no ser países asociados a los Estados Unidos de Norte América, los incidentes relacionados a ciberdelitos o ciberataques se encuentran monitoreados por el Observatorio de Ciberseguridad, el cual surge en colaboración de Banco Interamericano de Desarrollo BID por siglas en español y la Organización de los Estados Americanos OEA por sus siglas en español. Ya se han dado cuenta del aumento de ciberataques se vieron en la necesidad de implementar el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones CMM por sus siglas en inglés, con el fin de poder medir el crecimiento y el desarrollo de las capacidades de defenderse de las amenazas que surge en el ciberespacio.

En el Reporte de Ciberseguridad presentado por el BID y la OEA en el 2020, la República Dominicana por estar ubicada en la región del Caribe, de acuerdo al reporte está catalogada con un nivel de madurez de entre 1

y 2 en todas las dimensiones, este rango de madurez se encuentra definidos con un rango entre 1 y 5, donde la puntuación 1 significa que el país se encuentra implementando en una etapa inicial políticas y medidas de seguridad cibernéticas que permitan hacer frente a los ciberataques con métodos mucho más sofisticados y complejos, y la puntuación de 5 significa, que se encuentran en una etapa avanzada de la implementación de normas y medidas de seguridad establecidas dentro de la estrategia de ciberseguridad implementada. En este reporte mencionado anteriormente, se establecen indicadores como la cantidad de personas con acceso a internet al 2017 es de 7,103,852 es decir, el internet le llega al 68% de la población, que son aspectos importantes para tomar en consideración, ya que permiten realizar comparaciones de las condiciones en las que se encuentra el país respecto a otros países.

El cuerpo legal en la legislación dominicana que abarca los delitos cibernéticos es la Ley No. 53-07, referente a los Crímenes y Delitos de Alta Tecnología, en su artículo 17, regula el Robo de Identidad, el cual regula “El hecho de una persona valerse de una identidad ajena a la suya, a través de medios electrónicos, informáticos, telemáticos o de telecomunicaciones”. Con una redacción muy sencilla, queda claro que alguien al usar la identidad ajena, en las herramientas proporcionadas por el ciberespacio comete un delito. Lo parece que deja en ambigüedad es de

valerse para que, fuese la pregunta. Se entiende que las normas deben de ser redactadas de forma general, pero en este caso podría ser muy amplio.

Por ejemplo, existe el caso en que el Gerente General de una empresa le solicita a su secretaria que envié un correo desde su computadora a un proveedor, en el sentido estricto de la palabra la secretaria, en este caso hipotético, se está valiendo de la identidad ajena y estaría cometiendo un delito. Habría una significante diferencia si la redacción del artículo incluyera o hiciera referencia a que el fin de utilizar la identidad ajena es con propósito ilícito. Como lo establece el Convenio de Berna, es responsabilidad del legislador redactar los artículos que hagan falta para proteger los bienes jurídicos tutelados, en los casos que el convenio no haya establecido una recomendación. Es responsabilidad del legislador redactar los delitos desde un punto de vista general, pero concisos y que no se presten a malas interpretaciones.

Código Penal de Costa Rica

Costa Rica es uno de los países que cuenta con un territorio de 51,179 kilómetros cuadrados, una población total de 5,094,114, con un producto interno bruto de 61,85 mil millones de US$, el 99% tiene acceso a energía eléctrica y 81% de las personas tiene acceso a internet, datos reportados por el Banco Mundial al 2020. Es uno de los países con características

similares a Guatemala, ya solo con el hecho de pertenecer a la misma región Centroamericana, a pesar de que la liberación del comercio de la telefonía se realizó años después, de acuerdo con el Reporte de Ciberseguridad del 2020 realizado por el BID y la OEA, Costa Rica tiene un nivel de madurez en el ámbito de su marco legal y regulatorio entre 2 y 3, es decir, cuanta con reglas claras en el ámbito tecnológico y esto le permite brindar certeza jurídica a las instituciones internacionales. Esto sin duda alguna les ha abierto las puertas a que empresas tecnológicas muestren interés de establecer operación en el país y apoyen al incremento de trabajo, nivel educativo y la economía.

El Código Penal costarricense, regula en su artículo 230 el delito de Suplantación de Identidad, el cual establece lo siguiente, “Sera sancionado con pena de prisión de uno a tres años quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquier red social, sitio de internet, medio electrónico o tecnológico de información”. Este artículo se encuentra dentro de la sección octava, que referencia a los delitos informáticos y conexos, dichos delitos van de la mano de la política de ciberseguridad establecida por el gobierno, con el fin de proteger la seguridad de las personas y su propiedad en el ciberespacio. La integración del delito de suplantación de identidad o el espionaje cibernético en el código penal surge a raíz de la Ley 9048 emitida en el 2012 por el órgano legislativo.

En este caso, es mucho más específico en la forma de redactar del legislador, ya que se entiende que, la persona que utilice rasgos característicos en medios electrónicos, sitios de internet, o cualquier red social, estará cometiendo un delito. En donde toma en consideración de que los aspectos característicos de la identidad digital son aspectos diferenciadores de cada una de las personas y estos son parte del patrimonio de cada una de ellas. El artículo 230 establece que solo con el simple uso de símbolos característicos de la identidad de otra persona, deben de ser penado ya que se les está violentando la propiedad y conlleva a un sinfín de perjuicios a los que se verán afectados, entre ellos el daño de la reputación y daños psicológicos. De igual forma el delito contempla que el hecho de realizar la suplantación de identidad digital contempla que esta acción tiene como propósito el engaño, dañar la imagen, realizar estafas, obtener información de los usuarios con el fin de vulnerar la seguridad de otras plataformas.

Comparación de acciones típicas

Como se ha visto a lo largo de la presente investigación el delito de suplantación digital, es un delito el cual forma parte de las estrategias que cada uno de los países debe de acuñar con el propósito de resguardar distintos aspectos de la propiedad, propiedad que no únicamente le pertenece a la persona a la que le suplantaron la identidad, sino que en

términos generales tiene como resultado la vulneración de derechos de terceros que son consecuencia del delito primario. La implementación de estos delitos es la respuesta de los gobiernos a los métodos delictivos que los delincuentes están tomando frente al abanico de posibilidades que abre los avances tecnológicos y la interconexión de las personas a través de las redes sociales, el correo electrónico y los sitios en internet por mencionar algunos.

Países como Puerto Rico, República Dominicana y Costa Rica son países de Centro América y del Caribe que ya cuentan con legislación vigente que se encarga de tipificar el delito de suplantación de identidad digital, nombrado de distintas formas, de acuerdo con la percepción de cada uno de los legisladores, pero con un trasfondo en común, en la Tabla 1 se muestran las características de cada uno de las leyes vistas en el derecho comparado y los verbos rectores utilizados para describir las acciones que considero el legislador en cada uno de los países considerados para la presente investigación. Estos verbos son utilizados en distintos contextos y son sujetos a distintas interpretaciones.

Tabla 1

Cuadro de acciones típicas del delito de suplantación de identidad digital en el derecho comparado

Características	Puerto Rico	República Dominicana	Costa Rica
Cuerpo legal	Ley No. 146-2012 Código Penal	Ley No. 53-07 Crímenes y Delitos de Alta Tecnología	Código Penal
Artículo	209	17	230
Sujeto Activo	Cualquier persona	Cualquier persona	Cualquier persona
Sujeto Pasivo	Cualquier persona	Cualquier persona	Cualquier persona física, jurídica o de una marca comercial
Verbo rector	Apropie, con el propósito de realizar cualquier acto ilegal	Valerse	Suplante

El verbo apropie es utilizado con una segunda preposición la cual delimita la acción que el sujeto activo debe de realizar para que al realizar la acción sea punible. Por otro lado, valerse el diccionario de la real academia española lo describe un intransitivo patrimonial como servirse de algo o de alguien, utilizándolo para algún fin, en este caso el verbo está acompañado de una preposición que indica que el fin es hacer suya la identidad ajena. En el caso del verbo suplante o suplantar la Real

Academia Española establece que es “ocupar con malas artes el lugar de alguien, defraudándole el derecho, empleo o favor que disfrutaba”. Es decir, el termino suplantar enmarca la acción que el sujeto activo comete incluyendo el propósito que pretende logara, ya que establece lo que pretende afectar al sujeto pasivo.

Comparación de penas

Establecer las penas para las acciones típicas que son antijuridicas, es una de las herramientas más poderosas con las que cuenta el Estado para hacer valer sus regulaciones y están enfocadas en prevenir que estas acciones sean cometidas, de cierta forma intimidar a la población a no cometer actos delictivos. La pena es el resultado de como el estado valora la retribución que el sujeto activo debe de pagar por haber sido culpable de una acción típica y antijuridica. Lo cual es parte de la consecuencia y de todo lo que se debe de hacer para la reinserción social del sujeto activo. En la Tabla 2 se realiza una comparación de cómo cada uno de los Estados analizados, cuantifica la pena que un delincuente debe de pagar por realizar los actos de suplantación de identidad digital.

Tabla 2

Cuadro de penas de lo delito de suplantación de identidad digital en el derecho comparado

Descripción	Puerto Rico	República Dominicana	Costa Rica
Cuerpo legal	Ley No. 146-2012 Código Penal	Ley No. 53-07 Crímenes y Delitos de Alta Tecnología	Código Penal
Prisión	8 años	3 meses a 7 años	1 a 3 años
Multa		2 a 200 salarios mínimos	

En este punto es importante recordar los indicadores de cada uno de los países, en donde, cada uno de ellos permite darle una explicación a como cada uno de los Estados comparados valoran o perciben el derecho vulnerado, al cometer el delito de la suplantación de identidad. Puerto Rico que es un estado asociado de los Estados Unidos de Norte América, es en donde el 78% de la población usan internet y el que tiene el producto interno bruto más grande. Por otra parte, República Dominicana, en donde el 77% de la población usan internet, de cierta manera, la pena máxima es muy similar Puerto Rico, el órgano legislativo considero que aparte de sancionar con prisión también sancionara con multa que va desde 2 a 200 salarios mínimos.

Por último, Costa Rica es un país que recientemente incorpora el delito de suplantación digital, ha dado grandes pasos en comparación con los países centroamericana, es el país en donde el 81% de la población usan internet, pero, aun así, no perciben lo mismo que los países caribeños al momento de valorar como este delito puede llevar a perjudicar el patrimonio de las personas, ya que son quienes cuentan con las penas menores. Por consiguiente, es importante tomar en cuenta que de los tres países examinados, Costa Rica es el que cuenta con menor cantidad de producto interno bruto y otro dato interesante es que las remesas representan el 0.8% del producto interno bruto, según datos del Banco Mundial al 2020, en este caso podría decirse que la cantidad de transacciones financieras que se realizan a través de las distintas plataformas de pagos es muy poca y para tener un parámetro de referencia las remesas para la República Dominicana representan el 10.6% del producto interno bruto según datos del Banco Mundial al 2020.

Análisis de los efectos producidos en la propiedad por la suplantación digital en Guatemala y el Derecho Comparado

Estrategia Nacional de Ciberseguridad en Guatemala

La seguridad cibernética o ciberseguridad es un conjunto de prácticas acuñadas con el propósito de resguardar los activos de las personas en el ciberespacio, esto implica, garantizar la integridad y confidencialidad de la propiedad. Durante el 2018 Guatemala y la República Dominicana se unieron al grupo de países de la región de Centro América y el Caribe que publican su Estrategia Nacional de Seguridad Cibernética. Dicha estrategia, es parte de las acciones realizadas por Guatemala con el fin de generar las condiciones que garanticen los derechos humanos en el ciberespacio y son los pasos iniciales para establecer los lineamientos en orden de los requerimientos realizados en la resolución denominada "Adopción de una estrategia interamericana integral de seguridad cibernética: Un enfoque multidimensional y multidisciplinario para la creación de una cultura de seguridad cibernética" emitida por la Organización de los Estados Americanos. Resolución que surge de la sesión celebrada en Montevideo, Uruguay en enero del 2004, en donde se cuenta con el compromiso de identificar y combatir las amenazas a la seguridad cibernética y se insta a los Estados miembros a establecer una

red de cooperación a través de la implementación de centro unificado de seguridad de respuesta ante incidentes informáticos.

La Estrategia Nacional de Seguridad Cibernéticas, presentada por el Ministerio de Gobernación de Guatemala, está conformada de cinco capítulos. El primero de ellos es el diagnostico nacional sobre el estado de la ciberseguridad en Guatemala, en el segundo capítulo se establece la metodología para construcción de la estrategia adaptada de los organismos internacionales como la OEA y el Consejo de Europa, el capítulo número tres enmarca la visión y los principios fuentes de la Estrategia Nacional de Seguridad Cibernética, como cuarto punto se describen los ejes, objetivos y acciones alineados a la visión y principios establecidos, y por último el capítulo número cinco en donde establece la gobernanza de la seguridad cibernética alineada dentro del marco del Sistema Nacional de Seguridad.

Para comprender la necesidad de determinar porque es importante la seguridad cibernética, se deben de revisar los indicadores, los cuales permitirán comparar con países que se encuentren dentro de la misma región. En el caso de Guatemala cuenta con un territorio 108,889 kilómetros cuadrados, también los datos del Banco Mundial reportan que el producto interno bruto es de 77,6 mil millones de dólares americanos y que en el 2019 contaba con el 44% de la población con acceso a internet. A pesar de que Guatemala cuenta con un territorio y un producto interno

bruto mayor que Costa Rica, la cantidad de personas con acceso a internet es inferior, esto da la impresión de ser datos negativos, pero una de la explicaciones de él porque sucede esto, es que otros mercados, aparte de los que dependen de internet, son mucho más maduros y estos apoyan a tener una económica estable, el lado positivos de estos indicadores reflejan que hay grandes áreas de oportunidad para comercios que dependan del internet y es ahí en donde el gobierno debe de apoyar desde el marco legal para brindar certeza jurídica.

En Guatemala existen gran variedad de empresas que apoyan a la industria de la tecnología de la información, el internet y las comunicaciones. Por ejemplo, los bancos su giro de negocio se basa en productos financieros, pero todas las transacciones están respaldadas por sistemas de información que llevan los registros de cada una de las cuentas, hoy en día todo el sistema financiero se encuentra evolucionando por dos temas principalmente. El primero primer aspecto por el cual el sistema financiero se encuentra evolucionando son las criptomonedas las cuales está descentralizando la emisión de moneda y el intercambio de divisas a bajos costos, y como segundo aspecto, las empresas denominadas *fintech* que el termino en inglés hace referencia a servicios financieros basados en tecnología, en donde el principal beneficio que brindan es el acceso a servicios financieros a través aplicaciones que se comunican a través de

internet a sus proveedores, lo cual conlleva una mayor penetración del internet en la población.

Otro de los ejemplos son las empresas que se dedican a la prestación de servicios denominados *contact centers*, llamados así ya que son puntos de atención al cliente que prestan servicios a distintas compañías. En la actualidad la Agexport reporta 27 compañías asociadas que realizan actividades mercantiles de *contact center* y en el 2017 han realizado exportaciones desde Guatemala a otras partes del mundo, que tiene un valor de US$750 millones de dólares. Sin dejar de mencionar que en el 2019 generaron alrededor de 42,000 empleos. Estos son datos que permiten dar un panorama más amplio de la relevancia que esta toman el internet en Guatemala y de las repercusiones que puede tener el no prestarle la debida importancia a la certeza jurídica que el país debe de brindar y permita seguir impulsando este tipo de mercados.

Dentro de los requerimientos establecidos por la OEA, se encuentra la formación de un Equipo de Respuesta de Incidentes de Seguridad Informática denominado CSIRT por sus siglas en inglés *Computer Security Incident Response Team*. El CSIRT es el equivalente a la Red 24/7 establecido en el artículo 35 del Convenio de Budapest, que entre sus funciones se encuentran, ser el punto de contacto localizable las 24 horas del día, 7 días a la semana, ser el punto de asistencia inmediata para la

investigación de delitos vinculados a sistemas y datos informáticos, quien apoyara a obtener pruebas, conservara los datos, proveerá de información jurídica y localización de sospechosos y recolectara información con el objetivo de establecer datos estadísticos que documenten los incidentes, entre otros.

Entre los años 2010 y 2011 se iniciaron los primeros pasos para establecer la iniciativa CSIRT-gt el cual pretende ser el punto de contacto centralizados de la seguridad informática ante los organismos nacionales e internacionales en Guatemala. El funcionamiento ha sido limitado únicamente a ser utilizado por el Ministerio de Defensa, Ministerio de Relaciones exteriores, la Super Intendencia de Comunicaciones y asesores de seguridad independientes, la creación oficial aún se encuentra en proceso. Esto limita a la cantidad de información que se pueda tener respecto a las estadísticas de los tipos de ataques cibernéticos y a la cantidad de ocurrencias de cada uno de ellos en Guatemala.

Creación y utilización de perfiles falsos en redes sociales

Las redes sociales han ido incrementando con forme las necesidades de las personas de sociabilizarse en distintos ámbitos y como esto han ido evolucionando a lo largo del tiempo, hoy en día existen redes sociales de ocio, laborales, comerciales, entre otras. En general los perfiles en las

redes sociales están asociados a las cuentas de correo electrónico y únicamente se permite un perfil por cuenta de correo electrónico. Pero un dato muy importante es que cada persona ya sea física o jurídica puede llegar a tener cualquier cantidad de cuentas de correo electrónico, por consiguiente, estas personas podrían tener tantos perfiles en redes sociales como correos electrónicos y cada uno de ellos serían validos ya que cumplió con los requisitos indispensables para la creación de perfiles en cada una de las redes sociales.

La creación de perfiles falsos en redes sociales es un término subjetivo, ya que, los perfiles son creados por las personas y asociados a una cuenta de correo electrónico que efectivamente les pertenece. El problema se centra prácticamente en que los perfiles falsos, son los que quieren personificar ser otra persona y en este caso lo que hace es tomar imágenes representativas de la entidad que está tratando de suplantar. Es decir, que en esta imagen en donde la persona física o individual, invirtió tiempo, recursos y esfuerzo para la creación de la marca que se encuentra protegida por derechos de propiedad industrial, por componerse de un signo figurativo que identifica y distingue a una empresa. Y para la creación de este perfil falso no únicamente utiliza imágenes, sino que también utiliza el nombre con el propósito de engañar a los usuarios que utilizan las redes sociales.

Recientes estudios realizados por la firma de consultoría digital *iLifeBelt* en la publicación de su sitio web llamada, ¿Cuántos usuarios de Facebook hay en Guatemala?, con la última fecha de actualización en abril de 2021, revelan que en Guatemala hay 8.5 millones de usuarios en la red social denominada *Facebook* de los cuales 66% de usuarios mayores de 13 años, son audiencia potencial para interactuar con publicidad. Sabiendo esto las personas que utilizan los perfiles falsos contactan a los usuarios y valiéndose de ingeniería social, no solo por utilizar los rasgos distintivos sino porque utilizan métodos lingüísticos con los cuales pretenden obtener información que les permita quebrantar barreras de seguridad en otras plataformas, como los sitios de entidades financieras publicados en internet, o realizar compras usando datos de tarjetas de crédito que obtuvieron por medio de engaños.

El caso anterior, es la acción típica descrita en el Código Penal de Costa Rica, en donde se establece, quien suplante la identidad de una persona física, jurídica o de una marca comercial en cualquier red social está cometiendo un delito. Y es una práctica frecuentemente utilizada ya que *Facebook* u otras redes sociales, son un gran atractivo para los ciberdelincuentes por la cantidad de usuarios y la facilidad de contactar a cada uno de ellos. También dichas redes sociales cuentan con un sinfín de vulnerabilidades que permiten a los ciberdelincuentes tomar las imágenes y datos de los perfiles y hacerlos propios en perfiles, denominados falsos,

y de esta forma hacer caer por medio de engaños a personas que son vulnerables por no contar con medidas de seguridad.

No se cuentan con datos puntuales en Guatemala, pero en los Estados Unidos de Norte America este tipo de ciberdelito es denominado *Identity Theft*, la entidad *Internet Crime Compliant Center* denominada IC3, en su reporte *Internet Crime Report* del 2021 indica que por el delito de robo de identidad en el 2019 se contabilizaron 16,053 víctimas, en el 2020 de 43,330 y en el 2021 se llegó a alcanzar un total de 51,629 víctimas, lo cual han representado perdidas monetarias que ascienden a 278,267,918 millones de dólares americanos para las víctimas reportadas en el 2021. La constante creación de redes sociales podría ser una de las explicaciones del porque el valor de la cantidad de víctimas se ha incrementado, también depende mucho de las políticas de seguridad cibernética acuñada por las personas y como los Estados apoyen a brindar herramientas a los sistemas judiciales para la penalización de esta actividad.

Creación y utilización de mensajes electrónicos o páginas web, valiéndose de imágenes protegidas con derechos de propiedad intelectual simulando información de sitios conocidos

El correo electrónico y los sitios en internet son prácticamente las primeras funciones en internet tras su surgimiento, estos servicios permitían comunicar y difundir información a distancia de forma rápida, la cual se remota aproximadamente a los años sesenta, en donde es utilizado como instrumento para la comunicación entre los destacamentos militares. Con el paso del tiempo, estos servicios llegan a las universidades y en los años noventa con el surgimiento de las computadoras personales y siendo estas mucho más accesibles a las personas, el uso del correo electrónico y los sitios en internet se populariza a nivel mundial. Siendo utilizado no únicamente para comunicarse sino de forma comercial en donde contar con un sitio en internet o una cuenta de correo electrónico, para las empresas es contar con presencia y posicionamiento en el ciberespacio.

La popularidad del correo electrónico y de los sitios en internet vino de la mano de métodos para engañar a los usuarios como la ingeniería social, en donde, en estos casos la técnica utilizada está enfocada en difundir correos electrónicos tomando imágenes de instituciones financieras, tanto banco del sistema financiero guatemalteco, como la de aplicaciones denominadas billeteras electrónicas, las cuales son las que resguardan las

criptomonedas. Estos correos electrónicos no solo cuentan con imágenes, sino que solicitan a los usuarios que las claves de acceso sean restauradas y que esa operación puede realizarse fácilmente presionando un botón, el cual adjuntan dentro del correo electrónico. El siguiente paso se compone de dos opciones, la primera es descargar una aplicación la cual se analizarán las características en los siguientes títulos y la segunda opción es redirigir al usuario a un sitio internet, el cual es similar en todas sus características al sitio de la entidad financiera original. Pero obviamente este no es el sitio original y es un sitio de internet el cual tomo todos los elementos esenciales para engañar al usuario y hacerle pensar que se encuentra utilizando el servicio de la entidad en cuestión.

El usuario, quien no duda de la procedencia del correo electrónico y confía en el sitio al cual se dirigió, utiliza el sitio falso ingresando su cuenta de usuario y sus credenciales, dicho de otra forma, ingresa información como su clave de seguridad, que la víctima utiliza para autenticarse en las plataformas provistas por las entidades financieras, las cuales en ningún momento serán actualizadas como indicaban las instrucciones del correo electrónico falso que la víctima recibió. Esta información será almacenada en manos de los ciberdelincuentes, con el propósito de realizar transacciones que afectan el patrimonio de la víctima, por otro lado, indirectamente el patrimonio de las instituciones que los ciberdelincuentes suplantan se ve afectado, ya que, inconscientemente los usuarios dejan de

creer en dichas institución, destruyendo la reputación de estos, quienes deben de invertir grandes cantidades de dinero para implementar campañas publicitarias y aplicaciones de seguridad que apoyen a obtener la confianza de los clientes de nuevo y confíen en los servicios que ponen a la disposición de los usuarios.

En los Estados Unidos de Norte América este tipo de práctica es denominada *phishing* y de acuerdo con el informe *Internet Crime Report* del 2021 realizado por el *Internet Crime Complaint Center* denominado IC3, esta práctica en los últimos cinco años se ha incrementado exponencialmente, estimando 25,344 víctimas en el 2017 y llegando a alcanzar un total de 323,972 víctimas en el año 2021. El *phishing* es el método que cuenta con mayor cantidad de víctimas en los Estados Unidos de Norte América y en el 2021 represento 44,213,707 millones de dólares en pérdidas para las víctimas. La acción descrita en este apartado es muy ad hoc a como lo plantea la legislación de Puerto Rico, ya que hace referencia a quien se apropie de un medio de identificación de otra persona, en este caso se entiende que puede ser persona individual o jurídica, con el propósito de cometer cualquier acto ilegal, comete el delito de apropiación ilegal de identidad, regulado en el artículo 209 del Código Penal, Ley 146-2012.

Compra de artículos en internet valiéndose de información sustraída como resultado de engaño

La compra de artículos en internet es el resultado de los fraudes cometidos valiéndose de las actividades mencionadas en títulos anteriores, es la principal causa que motiva a los delincuentes a cometer dichas acciones, incrementar el patrimonio propio a costa de la disminución del patrimonio de las víctimas. Por ejemplo, en los últimos 10 años, las criptomonedas se han posicionados entre los artículos más cotizados por las personas, ya que fácilmente pueden ser utilizados como medios de pago y como activos de inversión. En donde no hay que contar con grandes cantidades de dinero para adquirir una criptomoneda y únicamente se necesitan billeteras virtuales para resguardarlos. Las billeteras virtuales, son proporcionadas por distintos proveedores en internet y estas billeteras son utilizadas dependiendo de la credibilidad de los proveedores.

Los delincuentes buscan apoderarse de las credenciales de las billeteras electrónicas, por la simple y sencilla razón que, sabiendo parámetros como la llave electrónica, permitirá el intercambio de criptomonedas, entre billeteras, sin que la transacción pueda ser rastreada, en este caso será a una de las múltiples billeteras electrónicas que posee el ciberdelincuente. Esto realmente parece irreal en la sociedad guatemalteca, pero en realidad es algo que está sucediendo a nivel mundial y a pesar de que las

criptomonedas al año 2022 no cuenten con una regulación específica en el ordenamiento jurídico guatemalteco, no es impedimento para que las criptomonedas sean utilizadas por la población y que sean un activo que es parte del patrimonio de las personas que viven en Guatemala.

Las transacciones que realizan los delincuentes a través de internet son múltiples, tan complejas con lo descrito referente a las criptomonedas, pero tan simple como adquirir el acceso a las cuentas de los sistemas financieros y realizar transferencias interbancarias o realizar pagos de servicios a cuentas ajenas, también podrían utilizar la información adquirida para gestionar compras de productos. Por otro lado, en Guatemala actualmente existe un amplio ecosistema de Fintech en proceso de desarrollo con ayuda de la Superintendencia de Bancos de Guatemala, quien pretende ser un punto de encuentro entre las entidades financieras supervisada y personas que desarrollan tecnologías financieras innovadoras. Las Fintech son intermediarios que prestan servicios financieros valiendo de sistemas de información publicados a través de internet, sin ser entidades bancarias, haciendo llegar servicios como formas de pagos a usuarios con acceso a un celular e internet. Esto da un panorama de la expectativa de crecimiento que el internet tendrá en Guatemala en los próximos años y como consecuencias es importante tomar la rienda de la seguridad cibernética ya que este tipo de

innovaciones conlleva a extenso abanico de vulnerabilidades que afectaran al usuario y a su patrimonio.

Acceso a documentos secretos sin la debida autorización

Anteriormente en el titulo referente a la creación y utilización de mensajes electrónicos o páginas web, se estableció que los ciberdelincuentes toman las imágenes protegidas por derechos de propiedad industrial y realizan una seria de mensajes electrónicos o sitios en internet que pretenden engañar al usuario para lograr dos objetivos. El objetivo que se pretende discutir en este apartado es en donde el ciberdelincuente pretende que el afectado descargue una aplicación la cual va escondida en un correo electrónico simulando ser de una institución conocida, en la cual le solicita que presione un botón o un hipervínculo adjuntado en el mismo correo. La victima al desconocer de buenas prácticas de seguridad cibernética, realiza lo que se le solicita en el cuerpo del correo y sin querer descargara una aplicación denominada *malware,* que también son llamados comúnmente virus y los cuales, se ejecutaran automáticamente en la computadora de la víctima, al está presionar el botón o el hipervínculo que se encontraba en el cuerpo del correo.

Al ejecutarse sin que la víctima se diera cuenta, el ciberdelincuente ha introducido un virus en su computadora el cual le abrirá las puertas y se esparcirá por toda la red interna a otras computadoras, sin importar si son de uso persona o de uso comercial. Esto les dará a múltiples opciones a los ciberdelincuentes para obligar a la víctima a pagar por el recate de la información secuestrada. Uno de los casos más conocidos son los virus denominados *Ransomware,* el cual es denominado así ya que es una aplicación que secuestra la información, el termino técnico correcto es que la información ha sido encriptada, con el objetivo de que la víctima no pueda ver sus propios archivos. Generalmente para liberar esta información hay dos opciones. La primera, que la víctima le page al ciberdelincuente una remuneración, generalmente es en criptomonedas, para proporcionar la llave para desencriptar y permita liberar la información. La segunda opción con la que cuenta la víctima es limpiar sus dispositivos de cualquier *malware*, generalmente si no cuenta con respaldos en este caso la información se perderá y deberá de cubrir los costos de recuperación para reconstruir la información perdida.

De acuerdo a los delitos que se describieron en el derecho comparado la suplantación de identidad conlleva el hecho de que los ciberdelincuentes toman imágenes, frases, signos distintivos, nombres comerciales, marcas, emblemas, entre otros para construir todo un correo electrónico y sitios en internet, que puedan engañar al usuario a proporcionar cuentas de accesos

o hacerlo caer en error y que ejecuten programas que abran las puertas, para capturar documentos o archivos digitales que cuenten con diseños industriales, invenciones, modelos de utilidad, procedimientos, registros, secretos empresariales, entro otros. Todo esto para hacer perder la credibilidad en las instituciones a las cuales están suplantado ya que deben de invertir en campañas publicitarias, sistemas de computadoras que permitan recobrar la confianza de sus usuarios y adicionalmente a una víctima que puede ser una persona física o jurídica y hagan perder horas de trabajo en la cual han invertido grandes cantidades de dinero para genera los archivos que han sido secuestrados y que adicionalmente incurran en gastos adicionales para recuperar la información.

Para tener una referencia, en los Estados Unidos de Norte América el departamento llamado *Internet Crime Complaint Center* denominado IC3 en su reporte *Internet Crime Report* del 2021, establece que a lo largo del año se han contabilizado 3,729 víctimas de *Ransomware* y 810 víctimas de *malware*/virus. Estos ataques han repercutido en el patrimonio de las víctimas y de acuerdo con el informe han representado 49,207,908 millones de dólares americanos en perdidas, sin tomar en consideración las pérdidas de lo negocio por el tiempo de recuperación de la información, o cualquier otro gasto al que las víctimas hayan tenido que incurrir, de igual forma las víctimas de ataques de *malware*/virus, se estima que han incurrido en 5,596,889 millones de dólares americanos en pérdidas.

Sustracción de propiedad industrial

Para explicar el hecho de que existe sustracción de la propiedad industrial al realizar la acción de suplantación de identidad digital, se presenta el siguiente silogismo, la primera premisa surge de entender, que la propiedad industrial está compuesta, entre otros por, emblemas, expresiones o señales de publicidad, marcas, nombres comerciales y signos distintivos. Y que estos atributos en el ciberespacio se convierten en parte de las características que identifican a una persona. Es decir, la identidad de las personas en el ciberespacio se compone de varios aspectos que son parte de la propiedad industrial.

La segunda premisa, surge de comprender que los delitos analizados en el derecho comparado establecen verbos como apropiarse, valerse, suplantar la identificación o identidad de una persona, con el propósito de realizar un acto ilegal. Los cual nos lleva a concluir que quien se apropie, o se haga valer o suplante, de la propiedad de una persona a través de medios electrónicos, con el propósito de realizar cualquier acto ilegal se encuentra cometiendo un delito y debe de atenerse a las consecuencias. Para ejemplificar el punto, se considera que una entidad financiera cuenta con un nombre comercial definido, señales publicitarias, marcas, emblemas, signos distintivos que lo identifican, pretende abrir perfiles en redes sociales con el objetivo de contar con presencia en el ciberespacio y un

ciberdelincuente toma todas estas características para crear un perfil falso, con el objetivo de engañar a los usuarios, esperando que alguno proporcione información que pueda ser utilizada para cometer un ilícito. En este momento el ciberdelincuente se encuentra suplantando la identidad digital de la entidad financiera, al realizar dicho acto daña la reputación y, en consecuencia, el patrimonio de dicha institución financiera. Por lo tanto, el ciberdelincuente debe de ser perseguido por las autoridades, no solo por engañar a la víctima valiéndose de las redes sociales, sino por, dignificar el buen nombre de la institución de suplanto.

Por otro lado, usando de nuevo como ejemplo a las entidades financieras, quienes crean correos con imágenes que los identifican por ser parte de su propiedad industrial y utilizan expresiones características en el cuerpo del correo, para comunicarse con sus usuarios o clientes y si los ciberdelincuentes toman estos correos y los difunden haciendo parecer que son las entidades financieras, creando cuentas de correos desde donde envían los mensajes y que tiene nombres de las entidades financieras, con un propósito de conseguir información que les permita cometer un ilícito, de igual forma se encuentran sustrayendo propiedad industrial al tomar estos signos distintivos. A parte de sustraer propiedad industrial por la creación de correos electrónicos falsos o la creación de perfiles falsos, también pueden llegar a sustraer propiedad industrial al lograr acceso a sistemas de información y capturar la información que de igual forma

pueden ser aspectos que se encuentran protegidos por la propiedad industrial.

La modalidad de estafa mediante whatsapp

Otra de las actividades que se ha popularizado en la actualidad es en donde el sujeto activo contacta al sujeto pasivo, por medio de *WhatsApp* haciéndose pasar por un familiar, por ejemplo, un supuesto familiar que se encuentra en problemas en un aeropuerto internacional, donde repentinamente debe de tomar otro vuelo y necesitan que alguien se haga cargo de su equipaje, el cual ya se fue en otro vuelo con destino a Guatemala. Para esto solicitan, que proporcionen información personal y un depósito de cierta cantidad de dinero a una cuenta bancaria, con el fin de que la maleta sea enviada por personal de la línea aérea una dirección en específico el estafador resuelve su situación migratoria. Este supuesto el cual es uno de los tantos que comúnmente utilizan, se evidencias que es otra forma de ingeniería social, con el objetivo de que la víctima realice algún depósito y proporcione información personal que les permita utilizar esta información al estafador, con fines delictivos.

Prensa Libre, uno de los diarios con mayor circulación del territorio guatemalteco, en su artículo denominado “MP ha recibido 602 denuncias por estafas por medio de WhatsApp” del día 14 de junio de 2022, por Sara Solórzano, reporta que, el número de quejas por estafa ha aumentado con

los años. De acuerdo con artículo, en el 2018 el Ministerio Público reporto 19 denuncia por estafa, en el 2019 se reportaron 88, mientras que en el 2020 el dato incremento a 458 denuncias y en el 2021 se presentaron 1,190 denuncias por estafa. Hay que tomar en consideración que el delito de estafa propio o los casos especiales de estafas, en ningún apartado consideran que las acciones sean valiéndose de medio tecnológicos. Es decir, los establecido en el Código Penal guatemalteco, en los artículos del 263 al 271, no se podría catalogar como ciberdelitos, ya que penalmente están prohibidos los tipos penales por analogía y en este caso no toman en consideración aspectos importantes para que estas acciones sean catalogadas como tales.

Además, el hecho de que en Guatemala este tipo de acción en contra del correcto actuar, no se encuentren debidamente tipificadas, con regulaciones que establezcan procedimiento de colaboración internacional y con un centro de atención nacional de alertas que categorice correctamente las denuncias. Se continuará con el aumento de denuncias que serán confundidas con tipos penales distintos y no se pondrán en acción practicas adecuadas para la investigación de este tipo de hecho o el resguardo de elementos de prueba. Y personas físicas, desde niños hasta adultos mayores se verán afectados en su patrimonio por estas prácticas que puede provenir tanto de personas que vivan en Guatemala como fuera de ella.

Conclusiones

Como resultado del objetivo específico uno planteado en la presente investigación, el cual se refiere a determinar, cuáles son los ciberdelitos que se encuentran tipificados en el ordenamiento jurídico guatemalteco y que aspectos de la propiedad vulneran las acciones descritas al ser ejecutadas por los ciberdelincuentes. Se concluyó que el Código Penal guatemalteco protege los registros y programas informáticos, la reproducción de programas de computación, la integridad de la información, el uso de información y los registros de un operador extranjero de telefonía, los cuales son considerado como parte del patrimonio de la persona y se encuentran regulados entre los artículos 274 A hasta el 274 H del Decreto número 17-73 de la Constitución Política de la República de Guatemala.

De conformidad con lo planteado en el objetivo específico número dos, el cual se refiere a examinar el abordaje de la suplantación digital en el Derecho Comparado. Se estableció que el Convenio Sobre la Ciberdelincuencia de Budapest promulgado por Consejo de Europa, en la actualidad es el documento que los Estados utilizan como referencia principal en la implementación de estatutos que regulen los ciberdelitos y los procedimientos que deben de crear para la colaboración internacional. Países como Puerto Rico, República Dominicana y Costa Rica, ya han

incluido en su ordenamiento jurídico el ciberdelito de suplantación de identidad digital, donde han señalado las acciones, típicas y antijuridicas, de acuerdo con la concepción de cada uno de sus legisladores, con el objetivo de resguardar el bien jurídico tutelado y fomentar la inversión de compañías de tecnología que apoyen al crecimiento económico de cada uno de esos países.

Respecto al objetivo general que tiene como objeto, relacionar cómo el delito de suplantación digital afecta jurídicamente la propiedad de las personas en Guatemala. Producto del hallazgo de la investigación se determinó que el delito de suplantación de identidad digital afecta de distintas formas el patrimonio de las personas. Primero el ciberdelincuente vulnera derechos de propiedad industrial de personas individuales o jurídicas, al valerse o apropiarse de elementos que son parte de la identidad digital de la víctima en el ciberespacio, por el simple hecho de hacer suyos signos distintivos, marcas, emblemas, entre otros. Con el objetivo de engañar a terceros, dañando la reputación, la honradez, el prestigio, del sujeto pasivo en el ciberespacio, daños que son cuantificables por indicadores como, la disminución de los ingresos, la cantidad de negociaciones futuras afectadas y la cantidad de inversión que se tiene que realizar para realizar nuevos negocios o restaurar los caídos. La segunda forma en que la propiedad de las personas se ve afectada es, cuando el sujeto pasivo cae en el engaño del sujeto activo, quien se valió de

ingeniería social, para acceder a cuentas o servicios en el ciberespacio y por medio de transacciones, sustrae el patrimonio de las víctimas o de terceros. Guatemala no está excluida de los ciberdelincuentes y mucho menos de los engaños por prácticas de suplantación de identidad digital, en muchos de los casos, las industrias que apoyan a la economía guatemalteca se encuentran conectadas a internet y utilizan medios tecnológicos para realizar sus operaciones. Por lo tanto, todas las personas con acceso a internet son parte del ecosistema denominado ciberespacio y sin importar el uso que se le dé a esta herramienta, son vulnerables a ser víctimas de hecho delictivos como el de la suplantación de identidad digital.

Referencias

Banco Mundial. (4 de abril de 2022). *Datos Costa Rica*. Recuperado de el 4 de abril de 2022 de https://datos.bancomundial.org/pais/costa-rica

Banco Mundial. (20 de Abril de 2022). *Datos Guatemala*. Recuperado de el 20 de abril de 2022 de: https://datos.bancomundial.org/pais/guatemala

Banco Mundial. (4 de Abril de 2022). *Datos Puerto Rico*. Recuperado de el 4 de abril de 2022 de https://datos.bancomundial.org/pais/puerto-rico

Banco Mundial. (4 de Abril de 2022). *Datos República Dominicana*. Recuperado de el el 4 de abril de 2022 de: https://datos.bancomundial.org/pais/República-dominicana

Barrio Andrés, M. (2017). *Ciberdelitos: amenazas criminales del ciberspacio.* Madrid: Cengage. https://elibro.net/es/ereader/upana/46673.

Comsición Interamericana de Telecomunicaciones. (Julio de 2004). *Resolución AG/RES. 2004 (XXXIV-O/04) "Adopción de una estrategia interamericana integral para combatir las amenazas a la seguridad cibernética: un enfoque multidimensionales y multidisciplinario para la creación de una cultura de seguridad cibernética".* Recuperada de Organización de los Estados Americanos: http://www.oas.org/en/citel/infocitel/julio-04/ult-ciberseguridad_e.asp

Conuncil of Europe. (s.f.). *Convenio sobre la ciberdelincuencia, informe explicativo.* Recuperado de el 19 de marzo de 2022 de https://rm.coe.int/16802fa403

De Mata Vela, J. F., & De León Velasco, H. A. (2016). *Derecho penal guatemalteco tomo II parte especial.* Magna Terra Editores.

Fernández Bermejo, D., & Martínez Atienza, G. (2020). *Ciberdelitos.* Ediciones Experiencia. Cengage Learning. https://elibro.net/es/ereader/upana/167811.

González Cauhapé-Cazaux, E. (2009). *Apuntes de derecho penal guatemalteco.* Guatemala: Fundación Myrna Mack.

iLifeBelt. (abril de 2021). *¿Cuántos usuarios de Facebook hay en Guatemala? [2021]*. Recuperado el 27 de abril de 2022 de: https://ilifebelt.com/cuantos-usuarios-de-facebook-hay-en-guatemala-datos-2018-2019/2018/11/#:~:text=De%20acuerdo%20con%20datos%20de,con%20publicidad%20desde%20esta%20plataforma

Internet Crime Compliant Center. (2021). *Internet Crime Report.* Recuperado el 25 de Abril de 2022 de https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf

Ministerio de Gobernación de la República de Guatemala. (24 de Abril de 2020). *Guatemala accede al Convenio sobre Ciberdelincuencia de Budapest*. Recuperado de Ministerio de Gobernación: 19 de marzo de 2022 de https://mingob.gob.gt/guatemala-accede-al-convenio-sobre-ciberdelincuencia-de-budapest/

Solórzano, S. (14 de Junio de 2022). MP ha recibido 602 denuncias por estafas por medio de WhatsApp. *Prensa Libre*. https://www.prensalibre.com/guatemala/justicia/mp-ha-recibido-602-denuncias-por-estafas-por-medio-de-whatsapp/

Legislación nacional

Asamblea Nacional Constituyente. (1985). *Constitución Política de la República de Guatemala.* Guatemala.

Congreso de la República de Guatemala. (1973). *Código Penal.* Decreto 17-73.

Congreso de República de Guatemala. (2000). *Ley de Propiedad Industrial.* Decreto número 57-2000.

Jefe de Goabierno de la República. (1963). *Código Civil.* Decreto Ley número 106.

Legislación internacional

Asamblea General de la ONU. (1948). *Declaración Universal de los Derechos Humanos.* Paris.

Congreso de la República de Puerto Rico. (2012). *Ley 146-2012 Código Penal.* Puerto Rico.

Congreso nacional de la República Dominicana. (2007). *Ley No. 53-07 Sobre crimen y delitos de alta tecnología.* Santo Domingo: Gaceta Oficial.

Council of Europe. (2001). *Convenio sobre la ciberdelincuencia.* Budapest: Los Estados miembros del Consejo de Europa.

La asamble legislativa de la república de Costa Rica. (1970). *Ley 4573 Codigo Penal.* Costa Rica: Sistema Costarricense de información Jurídica.

Organizacion de los Estados Americanos. (1969). *Convención Americana sobre Derechos Humanos.* San José.