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

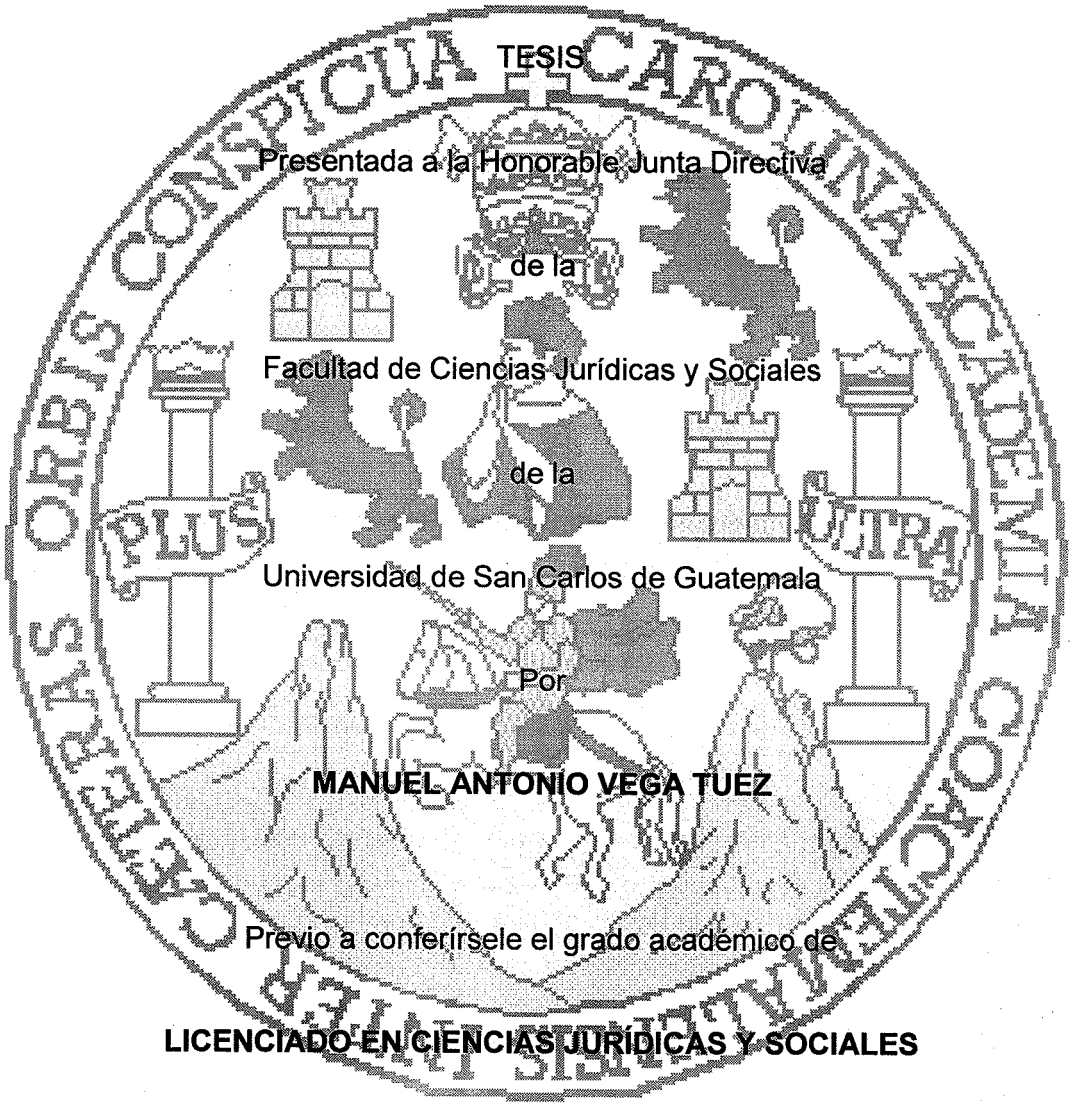
EVALUAR LA CREACIÓN DE UNA UNIDAD ESPECIALIZADA EN EL MINISTERIO PÚBLICO PARA PERSEGUIR LOS DELITOS CIBERNÉTICOS COMO LA ESTAFA DE INVERSIÓN EN CRIPTOMONEDAS

MANUEL ANTONIO VEGA TUEZ

GUATEMALA, ABRIL DE 2023

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

EVALUAR LA CREACIÓN DE UNA UNIDAD ESPECIALIZADA EN EL MINISTERIO PÚBLICO PARA PERSEGUIR LOS DELITOS CIBERNÉTICOS COMO LA ESTAFA DE INVERSIÓN EN CRIPTOMONEDAS



TESIS

Presentada a la Honorable Junta Directiva

de la

Facultad de Ciencias Jurídicas y Sociales

de la

Universidad de San Carlos de Guatemala

Por

MANUEL ANTONIO VEGA TUEZ

Previo a conferírsele el grado académico de

LICENCIADO EN CIENCIAS JURÍDICAS Y SOCIALES

Guatemala, abril de 2023

HONORABLE JUNTA DIRECTIVA

DE LA

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

DE LA

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

DECANO:	M.Sc. Henry Manuel Arríaga Contreras
VOCAL I:	Licda. Astrid Jeannette Lemus Rodríguez
VOCAL II:	Lic. Rodolfo Barahona Jácome
VOCAL III:	Lic. Helmer Rolando Reyes García
VOCAL IV:	Br. Javier Eduardo Sarmiento Cabrera
VOCAL V:	Br. Gustavo Adolfo Oroxom Aguilar
SECRETARIA:	Licda. Evelyn Johanna Chevez Juárez

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

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
GUATEMALA, C.A.

Facultad de Ciencias Jurídicas y Sociales, Unidad de Asesoría de Tesis. Ciudad de Guatemala, veintitres de marzo de dos mil veintiuno.

Atentamente pase al (a) Profesional, **ENMA LETICIA CASTELLANOS**, para que proceda a asesorar el trabajo de tesis del (a) estudiante **MANUEL ANTONIO VEGA TUEZ**, con carné **200010627**, intitulado **EVALUAR LA CREACIÓN DE UNA UNIDAD ESPECIALIZADA EN EL MINISTERIO PÚBLICO PARA PERSEGUIR LOS DELITOS CIBERNÉTICOS COMO LA ESTAFA DE INVERSIÓN EN CRIPTOMONEDAS.**

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

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

Adjunto encontrará el plan de tesis respectivo.

ASTRID JEANNETTE LEMUS RODRÍGUEZ
Vocal I en sustitución del Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
FAC. DE C.C. J.J. Y S.S.
UNIDAD DE ASESORIA DE TESIS
GUATEMALA, C. A.

Fecha de recepción 14 / 05 / 2021 f)

Licda. Enma Leticia Castellanos
ABOGADA Y NOTARIA

Asesor(a)
(Firma y Sello)

Guatemala 05 de agosto de 202

Jefe de la Unidad de Asesoría de Tesis
Facultad de Ciencias Jurídicas y Sociales
Universidad de San Carlos de Guatemala
Su despacho.

Distinguido Jefe de la Unidad:

Respetuosamente a usted informo sobre mi nombramiento como asesor de tesis de la Bachiller **MANUEL ANTONIO VEGA TUEZ**, la cual se intitula: **EVALUAR LA CREACIÓN DE UNA UNIDAD ESPECIALIZADA EN EL MINISTERIO PÚBLICO PARA PERSEGUIR LOS DELITOS CIBERNÉTICOS COMO LA ESTAFA DE INVERSIÓN EN CRIPTOMONEDAS**; declarando expresamente que no soy pariente del Bachiller dentro de los grados de ley; por lo que me complace manifestarle lo siguiente:

a) En el desarrollo de la revisión del trabajo de tesis relacionado, se discutieron algunos puntos en forma personal con el autor, realizándose los cambios y correcciones que la investigación requirió. La investigación busca demostrar que es necesaria la creación de una unidad especializada contra delitos cometidos mediante el uso de criptomonedas dentro del Ministerio Publico, ya que a la fecha no existe dicha unidad que coadyuve en la averiguación de la verdad por delitos cometidos por estafas con el uso de criptomonedas.

b) El sustentante utilizo métodos de investigación diversos, como lo son el método sintético, analítico, deductivo e inductivo, apoyado en las técnicas de investigación y bibliografía.

c) La redacción de la tesis es clara, concisa y explicativa, habiendo el Bachiller utilizado un lenguaje técnico y comprensible para el lector; asimismo, hizo uso de las reglas ortográficas de la Real Academia Española.

d) Se comprueba además que la bibliografía y técnicas de investigación utilizadas, fueron las adecuadas, puesto a que he guiado personalmente al sustentante durante el proceso de investigación científica, aplicando los métodos y técnicas apropiados para resolver la problemática esbozada con lo cual comprueba la hipótesis planteada conforme a la proyección científica de la investigación.

e) El Bachiller aceptó todas las sugerencias que se le hicieron y realizó las correcciones necesarias para una mejor comprensión del tema; en todo caso, se respetaron sus opiniones y los aportes que planteó.

f) Con base en lo anterior, hago de su conocimiento que la tesis cumple con todos los requisitos estipulados en el Articulo 31 del Normativo para la Elaboración de tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público, por lo que apruebo el trabajo de investigación, emitiendo para el efecto **DICTAMEN FAVORABLE**, para que la misma continúe el trámite correspondiente.

Respetuosamente;

Lcda. Enma Leticia Castellanos
ABOGADA Y NOTARIA

Lcda. Enma Leticia Castellanos
ABOGADA Y NOTARIA

Lcda. Enma Leticia Castellanos
ABOGADA Y NOTARIA

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
GUATEMALA, C.A.

Guatemala, 03 de noviembre de 2021

FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
RECIBIDO
03 NOV 2021
UNIDAD DE ASESORIA DE TESIS
Hora:
Firma:

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

Respetuosamente informo que procedí a revisar la tesis de el bachiller, **MANUEL ANTONIO VEGA TUEZ** la cual se titula **"EVALUAR LA CREACIÓN DE UNA UNIDAD ESPECIALIZADA EN EL MINISTERIO PÚBLICO PARA PERSEGUIR LOS DELITOS CIBERNETICOS COMO LA ESTAFA DE INVERSIÓN EN CRIPTOMONEDAS".**

Le recomendé al bachiller algunos cambios en la forma, estilo, gramática y redacción de la tesis, por lo que habiendo cumplido con los mismos emito **DICTAMEN FAVORABLE** para que se le otorgue la correspondiente orden de impresión.

Atentamente,

"ID Y ENSEÑAD A TODOS"

Licda. Brenda Margarita Martínez Cerna
Docente consejera de la Comisión de Estilo

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Decanatura de la Facultad de Ciencias Jurídicas y Sociales de la Universidad de San Carlos de Guatemala. Ciudad de Guatemala, diez de febrero de dos mil veintitrés.

Con vista en los dictámenes que anteceden, se autoriza la impresión del trabajo de tesis del estudiante MANUEL ANTONIO VEGA TUEZ, titulado EVALUAR LA CREACIÓN DE UNA UNIDAD ESPECIALIZADA EN EL MINISTERIO PÚBLICO PARA PERSEGUIR LOS DELITOS CIBERNÉTICOS COMO LA ESTAFA DE INVERSIÓN EN CRIPTOMONEDAS. Artículos: 31, 33 y 34 del Normativo para la Elaboración de Tesis de Licenciatura en Ciencias Jurídicas y Sociales y del Examen General Público.

CEHR/SAQO

DEDICATORIA

A DIOS: Quien, como guía, estuvo presente en el caminar de mi vida, bendiciéndome y dándome fuerzas para continuar con mis metras trazadas sin desfallecer.

A MIS PADRES: Manuel Antonio Vega Rodríguez y Juana Tuez Pérez, por ser el pilar fundamental en mi vida y demostrarme siempre su cariño y apoyo incondicional sin importar las adversidades.

A MI HERMANA: Ana Patricia, por su cariño y apoyo permanente durante todo este proceso y estar conmigo en todo momento.

A MI ESPOSA: Elizabeth, por ser el apoyo incondicional en mi vida, que, a través de tus concejos, amor y paciencia, alcance de mejor manera mis metas.

A MI HIJA: Gabriela Estefanía, tu afecto y tu cariño son los detonantes de mi felicidad, de mi esfuerzo, de mis ganas de buscar lo mejor para ti. Aun a tu corta edad, me has enseñado y me sigues enseñando muchas cosas de esta vida, te agradezco por ayudarme encontrar el lado dulce de la vida. Eres mi motivación más grande para concluir con éxito esta meta.

A MIS PADRINOS: Ana María Catalán Caceros y Gonzalo Alfonso Franco Paz, por su apoyo y ayuda a seguir adelante.

A LAS LICENCIADAS: Sara Leticia Sandoval Guerra, Alba Elizabeth Gudiel Pérez, Francis Rossmery Gómez Medrano, Irma Isabel Villafuerte

Duarte, Claudia Elizabeth Valladares Valladares y Elsa del Carmen Meza. Con admiración y ejemplo para alcanzar las metas de la vida.

A MI ASESOR: Lcda. Enma Leticia Castellanos, quien con su experiencia, conocimiento y motivación me oriento en el desarrollo de este trabajo de titulación.

A MIS AMIGOS: Lcda. Rosa Isabel Martínez Pérez, por su incansable colaboración y motivación para alcanzar este triunfo, y Marvin Arnoldo Ajuchan Cubur, un gran amigo, a quien le debo su apoyo incondicional.

A: Mi alma mater, Universidad de San Carlos de Guatemala y a la Facultad de Ciencias Jurídicas y Sociales, por haberme brindado tantas oportunidades y enriquecerme en conocimiento.

PRESENTACIÓN

La investigación que se realizó es sobre la evaluación de la creación de una unidad especializada en el Ministerio Público para perseguir los delitos cibernéticos como la estafa de inversión en criptomonedas, el objeto de estudio es determinar que tanto dentro del derecho sustantivo y adjetivo penal, no se cuenta con las herramientas para poder erradicar el delito en el territorio guatemalteco.

La amplitud del problema planteado estará dirigido desde el punto de vista de la disciplina jurídica del derecho procesal penal, porque se analizará la creación de una unidad especializada en el Ministerio Público que persiga los delitos cibernéticos como la estafa de inversión en criptomonedas y se profundizara en el estudio del derecho penal e investigación criminal al determinar aportes del Convenio sobre la Ciberdelincuencia de Budapest. El fenómeno objeto de estudio desde el punto de vista de su evolución diacrónica, se enfocó en el estudio de los antecedentes, y otros datos teóricos relacionados al tema, respecto a su aspecto sincrónico, se delimitó al estudio de los delitos cometidos en el ciberespacio.

El aporte que deja este informe está dirigido para proponer una serie de medidas que dé a conocer la necesidad de crear un ente dedicado a la investigación criminal de delitos informáticos y especialmente los realizados por estafas con criptomonedas, y pueda cubrir todo el territorio nacional y hacer cooperaciones internacionales para su eficacia y eficiencia investigativa.

HIPÓTESIS

Para poder determinar una protección jurídico penal que sancione los ilícitos penales de estafa cometidos en plataformas virtuales con criptomonedas, es necesario la creación de una unidad especializada en el Ministerio Público para perseguir los delitos cibernéticos como la estafa de inversión en criptomonedas y la legislación de un tipo penal tomando en consideración el modelo que propone el Convenio sobre la Ciberdelincuencia de Budapest, específicamente para hacer efectivo el Artículo ocho que establece el fraude informático.

COMPROBACIÓN DE LA HIPÓTESIS

El método deductivo permitió la comprobación de la hipótesis, en virtud de que se demostró que es necesaria la creación de una unidad especializada contra delitos cometidos mediante el uso de criptomonedas, dentro del Ministerio Público que coadyuve tanto a nivel interinstitucional, intrainstitucional e internacional en la averiguación de la verdad por delitos cometidos por estafas con el uso de criptomonedas y detectar las plataformas virtuales con apariencia de legalidad.

El objeto de estudio versa en que el Ministerio Público no cuenta con una unidad especializada en estos delitos y también no hay un tipo penal para sancionar hechos ilícitos cometidos con el uso de criptomonedas y existen personas que están cometiendo estafas mediante el uso de este tipo de monedas.

Por lo tanto, se propusieron una serie de bases para la implementación de la unidad, que legalmente debe cumplir cualquier unidad creada por el Ministerio Público, iniciado a través de la tramitación de un Acuerdo del Jefe de la institución, que forma las bases y órganos que deben organizar, coordinar, integrar y prestar el apoyo necesario para la creación de la unidad.

ÍNDICE

Pág.

Pág.

CAPÍTULO II

CAPÍTULO III

Pág.

CAPÍTULO IV

INTRODUCCIÓN

Las monedas criptográficas son medios privados y descentralizados de pago, paralelos al sistema monetario estatal. Son creados individualmente por los particulares y puestos en circulación por medio de distintas redes y medios de comunicación. La moneda criptográfica con mayor uso y popularidad es bitcoin, la cual puede ser utilizada para distintos servicios financieros. Este avance tecnológico ha permitido también la inclusión de comportamientos delictivos, siendo el espacio inmaterial cibernético el lugar de la comisión criminal, las legislaciones penales y procesales penales, no cuenta con las herramientas necesarias para su persecución y sanción.

El problema está centrado en establecer que el Ministerio Público no cuenta con una unidad especializada en estos delitos y también no hay un tipo penal que regule las actividades ilícitas cometidas mediante el uso de criptomonedas. A pesar de que a través del uso de las criptomonedas se pueden realizar distintas actividades ilícitas, en este sentido se determinaría la actividad ilícita, más no el uso de monedas criptográficas; asimismo, se han evidenciado casos de estafas en criptomonedas que se han realizado dentro del territorio guatemalteco.

La hipótesis se cumplió y los objetivos se alcanzaron al determinar una evaluación de la creación de una unidad especializada en el Ministerio Público, para perseguir los delitos cibernéticos como la estafa de inversión en criptomonedas. Además, se reflexionó sobre los aportes que da el Convenio sobre la Ciberdelincuencia de Budapest, tanto en la parte sustantiva como adjetiva penal.

El informe final del estudio está compuesto por cuatro capítulos, en los cuales se desarrollaron los siguientes temas: en el primero se describió las doctrinas sobre el derecho penal relacionado al problema planteado; en el segundo, se determinó la doctrina sobre los delitos informáticos; en el tercero, se analizó los ilícitos penales de estafa mediante el uso de criptomonedas; en el cuarto capítulo, se desarrolló la evaluación de la creación de una unidad especializada en el Ministerio Público para perseguir los delitos cibernéticos como la estafa de inversión en criptomonedas.

Los métodos de investigación utilizados, fueron: el sintético, analítico, deductivo e inductivo y las técnicas fueron el fichaje que entre ellas se encuentran las bibliográficas y de trabajo; asimismo, la revisión bibliográfica, hemerografía, documental, fueron parte también importante para el desarrollo de la tesis.

La investigación se realizó para establecer, en forma descriptiva-documental, la situación actual, tanto de la legislación penal, como de la investigación criminal sobre delitos de estafa cometidos mediante el uso de criptomonedas.

CAPÍTULO I

1. La teoría del delito

Para cualquiera de las partes, dentro del proceso penal, la teoría del delito es un método que le permite realizar un análisis de la conducta humana, considerada penalmente importante e indispensable para la resolución de los casos; su principal objetivo es, determinar si las conductas sujetas al proceso penal, encuadran dentro del concepto de delito; proporcionando para el efecto un camino lógico que permitirá identificar estas conductas.

1.1. Generalidades

La teoría del delito es una parte del derecho penal por medio del cual se estudia un conjunto de elementos que, estructurado lógicamente, permiten determinar si una conducta humana constituye o no, un delito. Esta estructura lógica es una serie de requisitos teóricos que permite determinar si un hecho puede establecer como delictivo. Los requisitos que permite determinar una conducta delictiva o no se denominan elementos, a su vez se dividen en positivos y negativos, cada uno de ellos entrelazados entre sí para poder examinar una conducta humana, es decir que si existe todos los elementos positivos se considera delito, pero si hay alguno negativo ya no lo es.

Los elementos positivos son: Acción, tipicidad, antijuridicidad, culpabilidad y punibilidad, mientras que los negativos son: falta de acción, atipicidad, causas de justificación, causas de inculpabilidad, falta de punibilidad.

1.2. Acción

Respecto a este elemento positivo del delito consiste en que es una conducta humana, activa o pasiva, voluntaria y que modifica el mundo exterior. Esta a su vez se divide en los siguientes elementos:

a) Conducta humana: solamente los seres humanos pueden cometer delitos.

b) Conducta activa o comisión: es faltar a un deber establecido por la ley penal de No Hacer.

c) Conducta pasiva u omisión: es faltar a un deber establecido por la ley penal de Hacer. La omisión puede ser: i) Propia o Simple Omisión: faltar a un deber genérico, un ejemplo de ello se encuentra en el Artículo 156 del Código Penal. ii) Impropia o Comisión por omisión: faltar a un deber específico. Esto se puede verificar en el Artículo 18 del anterior cuerpo legal citado.

d) Conducta voluntaria: se refiere a que la persona controle sus movimientos, que ninguna fuerza interna o externa influya en su conducta.

e) Modificación del mundo exterior: que no se quede solo en la mente de la persona, sino que lo debe exteriorizar.

La acción es el punto de partida de la existencia del delito y hay 2 teorías que la explican partiendo de diferentes puntos de vista:

a) Causalismo: la existencia de la acción, la tipicidad y la antijuridicidad es un resultado, en consecuencia, se modifica el mundo exterior. No importa su intención, sino solamente el elemento objetivo. El elemento subjetivo (intención), se analiza en la culpabilidad, no como un juicio de reproche, sino como algo psicológico del sujeto, capaz de comprender el hecho delictivo. La acción debe considerarse como la causa que produce el resultado prohibido.

b) Finalismo: indica que toda acción de ser humano siempre persigue un fin, en consecuencia, en la acción, tipicidad, antijuridicidad y culpabilidad, siempre debe observarse el elemento objetivo y el elemento subjetivo.

c) Teoría regulada en el Código Penal es la teoría de la causalidad adecuada, Artículo 10. "...Los hechos previstos en las figuras delictivas serán atribuidos al imputado, cuando fueren consecuencia de una acción u omisión normalmente idónea para producirlos, conforme a la naturaleza del respectivo delito y a las circunstancias concretas del caso o cuando la ley expresamente los establece como consecuencia de determinada conducta."

1.3. Falta de acción

La contraparte del elemento positivo de la acción, es la falta de ella y pertenece a un elemento negativo de la teoría del delito que hace que no exista acción por la falta de voluntad del sujeto que lo realiza, en virtud de existir movimientos reflejos; fuerza física irresistible y estado de inconsciencia no buscado de propósito. Este a su vez se subdivide en los siguientes elementos:

a) Movimientos reflejos: son movimientos involuntarios que realiza el cuerpo, provocados por estímulos internos o externos, que no se pueden controlar.

b) Fuerza física irresistible: es una fuerza material que recae sobre la persona que provoca realizar la conducta. Este se encuentra dispuesto en el Artículo 25 del Código Penal, asimismo esta se puede clasificar en dos: la primera física o vis absoluta: fuerza que recae directamente sobre el cuerpo de la persona que provoca la conducta que realizó, la voluntad es nula. Por ejemplo, en accidentes provocados por un desastre natural. La segunda Psicológica o vis compulsiva: fuerza que recae sobre la mente de la persona que consiste en amenazarlo con hacerle daño, lo que provoca miedo invencible. Artículo 25 numeral uno del Código Penal.

c) Estado de inconsciencia no buscado de propósito: Los órganos sensoriales o sentidos, se desconectan con el cerebro, ya no envían la información que reciben, por lo que la persona actúa sin voluntad, este tipo de comportamiento lo regula el Artículo 23 numeral dos del Código Penal, y frecuentemente son ejemplificados con

una persona que realiza una acción inconsciente porque está enferma, sonámbula o bajo los efectos de una hipnosis.

1.4. Tipicidad

La tipicidad es un elemento positivo de la teoría del delito que consiste en encuadrar la acción a un tipo penal, este es la descripción de una conducta delictiva dentro de la ley penal donde se encuentran acciones prohibidas, también se encuentra el concepto de tipificar, pero se le atribuye a la actividad legislativa por la que se criminaliza una conducta humana.

1.4.1. Funciones del tipo penal

Las funciones del tipo penal son las siguientes:

a) Función seleccionadora: el Estado selecciona las conductas que prohibirá, están contenidas en la ley penal.

b) Función motivadora: el estado obliga a las personas a comportarse de manera determinada, a no violar la ley.

c) Función garantizadora: garantía criminal y penal del principio de legalidad; si no existe el tipo penal para una acción, no se puede sancionar la misma.

1.4.2. Elementos del tipo penal

Los elementos del tipo penal son los siguientes:

a) Elemento Objetivo: es la descripción que hace el tipo penal de conductas externas.

b) Elemento Subjetivo: es la descripción que hace el tipo penal sobre la intención con que se realizó la conducta externa (con o sin intención). Pueden ser: Dolo culpa o preterintencionalidad.

Respecto al dolo este se encuentra regulado en el Artículo 11 del Código Penal, se considera que es un elemento subjetivo del tipo penal, que consiste en una intención deliberada para poder llegar a un fin, propósito o resultado, esto pueden ser: i) Directo: realizar una acción para producir un daño, ii) eventual: no persigue ese resultado en especial, pero sabe que lo conseguirá producto de su acción.

Otro elemento subjetivo del tipo penal es la culpa, se encuentra regulado en el Artículo 12 del Código Penal, consiste en causar un daño sin la intención de producirlo, pero se produce por: i) Negligencia: falta de cuidado antes de la acción, ii) Imprudencia: falta de cuidado durante la acción, iii) Impericia: falta de cuidado por no tener el conocimiento necesario.

El tercer elemento subjetivo del tipo penal es la preterintencionalidad, se encuentra regulado dentro del Artículo 26 numeral seis del Código Penal, consiste en la intención de causar un daño, pero no de tanta gravedad, como el que se produjo (intermedio

entre dolo y culpa). Un ejemplo de ello es disparar al aire para intimidar y la bala perdida hiere a una persona.

Es importante que, para considerar un comportamiento como delito a través del examen del tipo penal, debe de existir tanto el elemento objetivo y subjetivo del mismo. También dentro del estudio de los elementos subjetivos del tipo penal, se encuentra la figura del caso fortuito que la liberación de la responsabilidad penal si las acciones u omisiones lícitas, observando la debida diligencia, produzca un resultado dañoso por mero accidente, en estos casos no hay dolo ni culpa, (Artículo 22 del Código Penal).

1.5. Atipicidad

La atipicidad es el elemento negativo de la teoría del delito que consiste en determinar que una acción, no está prohibida por la ley penal, no encuadra en el elemento objetivo, ni en el elemento subjetivo, descrito en título anterior.

1.6. Antijuridicidad

La antijuridicidad es el elemento positivo de la teoría del delito, que consiste en que la acción, típica, es contraria al ordenamiento jurídico en su conjunto, por no existir causa que la justifique. La diferencia entre la tipicidad y la antijuridicidad es: toda acción antijurídica es típica, pero no toda acción típica es antijurídica.

1.7. Causas de justificación

Las causas de justificación es el elemento negativo de la teoría del delito, que consiste en normas permisibles para cometer una acción, típica. La clasificación de este concepto se encuentra dispuesto en el Artículo 24 del Código Penal, los cuales son:

1.7.1. Legítima defensa

Es una causa de justificación realizada por quien obra en defensa de su persona, bienes o derechos, o en defensa de la persona, bienes o derechos de otra. Siempre que concurran las siguientes circunstancias: i) Agresión ilegítima: la agresión recibida es típica y antijurídica, no hay causa que la justifique. ii) Necesidad racional del medio empleado para impedirla o repelerla: no necesariamente hay relación entre la racionalidad y la proporcionalidad. iii) Falta de provocación suficiente por parte del defensor. Existen dos modalidades de legítima defensa regulada dentro del Código Penal, estas son:

a) Legítima defensa privilegiada: Tiene lugar cuando un morador rechaza al que pretenda entrar o haya entrado en morada ajena o en sus dependencias, y realiza alguna acción para evitarlo. (Artículo 24 numeral uno, literal C, del Código Penal).

b) Legítima defensa putativa: consiste en ejecutar el hecho en la creencia racional de que existe una agresión ilegítima contra su persona, siempre que la reacción sea en proporción al riesgo supuesto. (Artículo 25, numeral tres, del Código Penal).

1.7.2. Estado de necesidad

Esta es una causa de justificación que tiene lugar cuando se daña un bien jurídico para salvar otro, en las circunstancias que señala la ley, las cuales son: i) Defensivo: se dañan bienes jurídicos del sujeto que está en peligro. ii) Agresivo: se daña un bien ajeno al sujeto que está en peligro. iii) Justificante: se daña un bien jurídico de menor valor en relación al otro que se salva. iv) Disculpaste: se daña un bien jurídico de mayor o igual valor en relación al que se salva. Se considera que no hay estado de necesidad: cuando las personas tienen el deber de afrontarlo o sacrificarse.

1.7.3. Legítimo ejercicio de un derecho o el cumplimiento de una obligación

El legítimo ejercicio de un derecho o el cumplimiento de una obligación es una causa de justificación que consiste en actuar en el legítimo ejercicio de un derecho o en el legítimo cumplimiento de una obligación.

1.8. Culpabilidad

La culpabilidad es el elemento positivo de la teoría del delito que consiste en un juicio de reproche de la sociedad que se le hace a una persona que cometió una acción, típica y antijurídica, y tubo las posibilidades de comportarse de otra manera. Este elemento se relaciona con el Principio de Culpabilidad: nadie puede ser sancionado, sin ser declarado culpable, (Artículo ocho de la Convención Americana sobre Derechos Humanos). Sus elementos y fundamentos son:

a) Capacidad para comprender el tipo penal: Capacidad mental para comprender la acción típica y antijurídica, debe ser una persona estable psicológicamente y mayor de edad.

b) Exigibilidad de comportamiento distinto: Que a la persona se le pueda exigir un comportamiento distinto a la acción, típica y antijurídica que cometió; no hay causas de exculpación.

c) Que conozca el tipo penal: que no ignore el tipo penal; esto decretado en el Artículo tres de la Ley del Organismo Judicial, donde exponencialmente establece que no se puede alegar ignorancia de la ley.

1.9. Causas de inculpabilidad

El elemento negativo de la culpabilidad es la inculpabilidad, indica que una persona que comete una acción, típica y antijurídica, no pudo comportarse de otra manera, es decir no existió otra opción para poder evitar su acción. Doctrinariamente se clasifican en:

1.9.1. Inimputabilidad

Regulada en el Artículo 23 del Código Penal, este precepto considera que una persona inimputable es la que no tiene la capacidad de comprender un injusto penal: i) Por ser menor de edad. ii) Por enfermedad mental, desarrollo síquico incompleto o retardado o trastorno mental transitorio, salvo que el trastorno mental transitorio, haya sido buscado de propósito por el agente (actio libera in causa).

1.9.2. Causas de exculpación o inculpabilidad

Las causas de exculpación o inculpabilidad se encuentran reguladas en el Artículo 25 del Código Penal estas causas que hacen que a una persona no se le pueda exigir un comportamiento distinto, (la sociedad también hubiera hecho lo mismo), siendo las siguientes:

a) Miedo invencible: Es actuar por miedo invencible de un daño igual o mayor, cierto o inminente.

b) Fuerza exterior: Es actuar violentado por fuerza material exterior irresistible, directamente empleada sobre él.

c) Error: Es ejecutar el hecho en la creencia racional de que existe una agresión ilegítima contra su persona, siempre que la reacción sea en proporción al riesgo supuesto (legítima defensa putativa).

d) Obediencia debida: Se considera como tal, cuando reúna las siguientes condiciones (sin perjuicio de la responsabilidad correspondiente a quien lo haya ordenado): i) Que haya subordinación jerárquica entre quien ordena y quien ejecuta el acto; ii) Que la orden se dicte dentro del ámbito de las atribuciones de quien la emite, y esté revestida de las formalidades legales; iii) Que la ilegalidad del mandato no sea manifiesta.

e) Omisión justificada: incurrir en omisión por no poder actuar, por causa legítima e insuperable.

1.9.3. Error de prohibición

El error de prohibición es una causa de inculpabilidad y es el desconocimiento que se tiene sobre la norma jurídica que la prohíbe. Dentro del Código Penal es un atenuante regulado en el Artículo 26 del numeral nueve del Código Penal. Su clasificación es la siguiente:

a) Error de tipo: se confunden algunos elementos del tipo penal. Esto regulado en el Artículo 173, segundo párrafo, Código Penal.

b) Error en persona: Se encuentra dispuesto en el Artículo 21 del Código Penal y establece de quien comete un delito es responsable de él, aunque su acción recaiga en persona distinta a aquella a quien se proponía ofender.

c) Error en golpe: Fundamento dentro del Artículo 21 del Código Penal, en su último párrafo, establece que: Quien comete un delito es responsable de él aunque... el mal causado sea distinto del que se proponía ejecutar. (Aberratio Ictus).

1.10. Punibilidad

La punibilidad es un elemento de la teoría del delito que consiste en que la acción, típica, antijurídica, culpable y punible, debe estar sancionada por la ley. Este elemento positivo de la teoría del delito se encuentra en discusión si es o no parte de esta teoría, existen dos criterios doctrinarios al respecto:

a) En un criterio, sí se considera que es un elemento positivo de la teoría del delito se necesita de este (además de la acción, típica, antijurídica y culpable) para considerar una conducta como delito.

b) En el otro criterio, se considera que es una consecuencia del delito. También se considera que el delito es solo la acción; típica; antijurídica y culpable. Que a veces tiene pena y a veces no (punibilidad).

1.11. Falta de punibilidad

La falta de punibilidad es un elemento negativo de la teoría del delito que consiste en que la acción, típica, antijurídica y culpable, no es punible o puede dejar de serlo, para ello se deben establecerse:

1.11.1. Condiciones objetivas de punibilidad

Son necesarias para imponer una pena o iniciar su imposición, que si desaparecen no hay posibilidad de imponer una pena. Para que exista la falta de punibilidad, debe haber falta de condiciones objetivas de punibilidad, un ejemplo de ello es la negación de asistencia económica, descrita en los Artículos 242 al 245 del Código Penal, se exime de la sanción quien haga efectivo el pago y garantice su futuro cumplimiento.

1.11.2. Excusa absolutoria

El legislador señala los casos en que no procede la imposición de una pena atendiendo a una política criminal según de cada delito o caso especial, encontrándose los siguientes ejemplos:

a) En el caso de delito de hurto regulado en el Artículo 246 del Código penal, tiene también dispuesto en el Artículo 280 del mismo cuerpo legal causas a quiénes están exentos de responsabilidad penal, aunque tengan responsabilidad civil que son: cónyuge, conviviente, hermanos.

b) No constituyen delito o falta las publicaciones que contengan denuncias, críticas o imputaciones contra funcionarios o empleados públicos por actos efectuados en el ejercicio de sus cargos. (Artículo 35 segundo párrafo de la Constitución Política de la República de Guatemala)

c) También el delito de rebelión o sedición regulado en el Artículo 388 del Código Penal tiene una exención, este se encuentra en el Artículo 476 del mismo cuerpo legal citado, y establece la exención de la pena por encubrimiento. iv) Puede ser la Pena Natural: que el inculpado haya sido afectado directa y gravemente por las consecuencias de un delito culposo y la pena resulte inapropiada. (Artículo 25, numeral cinco del Decreto Número 51-92 del Congreso de la República de Guatemala)

1.12. Consecuencia jurídica del delito

Las consecuencias en la comisión de un hecho delictivo es la imposición de una sanción, esta puede ser penal a través de una pena de prisión, medida seguridad o multa y también se derivan responsabilidades civiles como: restitución, reparación de daños materiales y morales y la indemnización de daños y perjuicios.


FACULTAD DE CIENCIAS JURIDICAS Y SOCIALES
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
GUATEMALA, C.A.

CAPÍTULO II

2. Delitos informáticos

Desde el año 1995 Guatemala empezó a introducir la automatización a través de programas computarizados, en esa época quien tenía la posibilidad de accesar a la tecnología era entidades bancarias y empresas multinacionales, los centros educativos recién estaban introduciendo en sus currículos de estudios la capacitación o el diplomado en computación, que conforme pasaba el tiempo fue siendo parte de la vida cotidiana de los ciudadanos, hasta el punto que hoy en día hay por lo menos un computador o un teléfono inteligente se encuentra en cada hogar guatemalteco que les permite el ingresar al ciberespacio.

Ese acceso al mundo informático ha permitido que cada ciudadano guatemalteco sea parte del ciberespacio, esta transformación en la comunicación o interacción humana, abrió paso al comercio electrónico y a las transacción financiera, provocando también una transformación en hechos delictivos, tanto en el mundo material como el inmaterial como lo es la internet, convirtiéndose en los denominados delitos informáticos, donde su ámbito territorial es inmaterial pero con consecuencias económicas materiales y psicológicas.

2.1. Breve reseña histórica

La implementación de la tecnología ha creado una nueva sociedad, aunque esta tiene una plataforma inmaterial o virtual, está siendo la base para crear interacciones humanas cada vez más consolidadas que han permitido nuevas formas de

comunicación social, relaciones humanas, comerciales, económicas y financieras entre otras, es tan rápido su avance que los Estados Nación en su tutela ciudadana no han podido avanzar, sin embargo es inminente que puedan crear leyes especiales que cubran estos ámbitos cibernéticos.

En el ámbito del Derecho Penal, "...se ha visto en la necesidad de normar ámbitos de protección a bienes jurídicos tutelados que anteriormente no existían o no se consideraban merecedores de defensa estatal. En ese sentido se puede ubicar cronológicamente el siglo veinte, como el origen y evolución de los delitos de carácter informático". Los ataques al programa o sistema operativo de un computador pueden ser considerados como las primeras conductas merecedoras de regulación y sanción de carácter penal".[1]

Respecto a actos que causaban daño en sistemas informáticos en el año 1959 en los Estados Unidos de América se presentó un caso donde tres programadores Robert Thomas Morris, Douglas McIlory y Víctor Vysottsky, de la compañía Bell Computer crearon un sistema llamado Corewar, este programa provocaba que la memoria de un computador fuera disminuyendo lentamente hasta que se acabara por completo.

Otras de las formas delictivas dentro de sistemas informáticos son los virus, y uno de los primeros "...aparece en el año de 1972, y se le denominó Creeper (enredadera en idioma inglés), que afectó a las computadoras de la compañía IBM e hizo necesaria la aparición del primer antivirus conocido como cegadora. Posteriormente en el año 1980

[1] Noriega Salazar, Hans Aarón. **Delitos Informáticos**. Pág. 21

el Arpanet, (sistema de comunicación vía computadoras usado por el departamento de defensa de los Estados Unidos y precursor de Internet), experimentó ataques a través de un virus informático que necesitó de tres días de trabajo para eliminarlo".[2]

Conforme paso el tiempo fue necesario que entidades internacionales empezaran abordar los problemas que se presentaban en el ciberespacio, es así que la Organización de Cooperación y Desarrollo Económico (OCDE), realizo estudios a partir del año 1983 para la creación de una legislación penal con el fin de combatir programas informáticos de uso indebido.

Los logros realizados derivados del análisis fue la publicación de un documento que se denominó Delitos de Informática análisis de la normativa jurídica, donde se describía un compendio de normas criminales vigentes y su propuesta para adaptarlas a través de reformas a la legislación de los Estados parte, así como nuevas conductas que se consideraban delitos y que debían sancionarse, esto fue considerado como una lista mínima, la cual en el futuro fue ampliada.

En el caso de Guatemala los delitos informáticos fueron abordados a partir del año 1996 entre ellos se encontraba la destrucción de registros informáticos, alteración de programas y la reproducción de instrucciones o programas de computación entre otros.

[2] **Ibíd.**, Pág. 22

2.2. Definición

Según el autor Barrios Osorio, define: "...de forma básica como delito informático las acciones prohibidas por la ley, cometidas en contra de uno o varios de los elementos que integran un sistema de información o los derechos que del mismo se deriven (protección de datos, intimidad o privacidad, derechos de autor)". Gabriel Andrés Cámpoli citado por Barrios Osorio define como delitos informáticos electrónicos "en los cuales el autor produce un daño o intromisión no autorizada en aparatos electrónicos ajenos... pero que poseen como bien jurídico tutelado en forma específica la integridad física y lógica de los equipos electrónicos y la intimidad de sus propietarios".[3]

La informática es definida en el Diccionario de la Real Academia de la Lengua Española como "el conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de ordenadores".[4] La Organización de las Naciones Unidas al referirse a la delincuencia informática lo hace de la siguiente manera: "A menudo, se le considera una conducta proscrita por la legislación y/o la jurisprudencia, que implica la utilización de tecnologías digitales en la comisión del delito; se dirige a las propias tecnologías de la computación y las comunicaciones; o incluye la utilización incidental de computadoras en la comisión de otros delitos".[5]

[3] Barrios Osorio, Omar Ricardo. **Introducción de las nuevas tecnologías en el Derecho.** Pág. 147
[4] http://www.rae.es/ (Consultado el 2 de julio de 2021)
[5] http://www.onu.org.gt/, (Consultado el 2 de julio de 2021)

2.3. Ámbito espacial de los delitos informáticos

El ámbito espacial o el territorio donde se comete los delitos informáticos es de vital importancia ya que los delitos son juzgados por las leyes del territorio donde se han cometido, en virtud que las leyes criminales o la forma de juzgarlas no es igual en todos los países, la internet o el ciberespacio, es la intercomunicación constante de personas de distintos países, asimismo las transacciones económicas o comerciales también se han transformado y por lo tanto la extraterritorialidad de la ley es inminente.

El Código Penal establece el principio de territorialidad en su Artículo 4, estableciendo que: "Salvo lo establecido en tratados internacionales, este Código se aplicará a toda persona que cometa delito o falta en el territorio de la República o en lugares o vehículos sometidos a su jurisdicción."

En relación a la extraterritorialidad de la ley penal también el Código Penal lo aborda en su Artículo cinco, estableciendo que la ley penal se aplicará en los siguientes casos extraterritoriales:

a) Por delito cometido en el extranjero por funcionario al servicio de la República, cuando no hubiere sido juzgado en el país en el que se perpetró el hecho.

b) Por delito cometido en nave, aeronave o cualquier otro medio de transporte guatemalteco, cuando no hubiere sido juzgado en el país en el que se cometió el delito.

c) Por delito cometido por guatemalteco, en el extranjero, cuando se hubiere denegado su extradición.

d) Por delito cometido en el extranjero contra guatemalteco, cuando no hubiere sido juzgado en el país de su perpetración, siempre que hubiere acusación de parte o del Ministerio Público y el imputado se hallare en Guatemala.

e) Por delito que, por tratado o convención, deba sancionarse en Guatemala, aun cuando no hubiere sido cometido en su territorio.

f) Por delito cometido en el extranjero contra la seguridad del Estado, el orden constitucional, la integridad de su territorio, así como falsificación de la firma del Presidente de la República, falsificación de moneda o de billetes de banco, de curso legal, bonos y demás títulos y documentos de crédito.

A pesar de que la ley guatemalteca prevé la extraterritorialidad de la aplicación de la ley, no se ha determinado la aplicación multiterritorial de la normativa criminal, en virtud de que los delitos cometidos en el ciberespacio, conlleva muchas veces a ordenadores que se encuentran en distintos países para la comisión de un hecho delictivo, creando de esta manera nuevos términos como ciber delitos, delitos informáticos, delitos electrónicos, delitos cibernéticos, etc., para poder abarcar comportamientos acordes a las nuevas tecnologías.

2.4. La responsabilidad en la comisión de un delito

Las consecuencias jurídicas de la comisión de un hecho delictivo realizado en medios informáticos es el mismo que se realiza con otros delitos, siendo responsabilidades civiles y penales.

Las responsabilidades penales son a través de las sanciones la imposición de una pena de prisión o multa, o medida de seguridad, mientras que en el ámbito civil es el resarcimiento económico que debe hacer el condenado por un hecho ilícito, o la persona que la ley señale como culpable, denominado tercero civilmente demandado, a la víctima o agraviada de la comisión del hecho delictivo.

2.5. Elementos que componen los delitos informáticos

Para determinar la comisión de un hecho delictivo en el ciberespacio, es necesario tener una base para que sea posible concretarlo, es decir que estos delitos a diferencia de otros deben existir elementos accesorios como es el computador con un sistema capaz de transmitir información y que pueda a su vez ser receptor de la misma. Se pueden dividir en dos los elementos de los delitos informativos, el primero es inmaterial, que es el sistema de información y el segundo material que es el equipo que se utiliza para la transmisión.

En relación al sistema de información es un conjunto de datos administrados, recolectados, recuperados, procesados, almacenados y distribuidos, para lograr un fin común, que puede ser la prestación de un servicio, proporcionar información o

transmitir datos, denominado también software o programas del ordenador, mientras que el elemento material se denomina hardware o el equipo de computación.

2.6. Bien jurídico tutelado

Los bienes jurídicamente tutelados son comportamiento normados en la Ley Penal, considerados como valores que el Estado debe proteger y amparar, en virtud de que causan serios daños a la sociedad, la fuente y el origen de cada uno puede ser histórico, social, cultural según la dinámica del comportamiento humano en la sociedad.

Se determinó en párrafos anteriores que los primero daños a la sociedad que produjeron los delitos informáticos eran a los sistemas a través de la creación de virus, sin embargo con el paso del tiempo los hechos ilícitos empezaron a transgredir otros comportamiento, como patrimoniales en el caso de robos al sistema bancario y de datos que permitan el acceso a cuentas o tarjetas de crédito, a la honor cuando a través de redes sociales se difama a una persona, en el caso de delitos sexuales informáticos, como por ejemplo la pornografía infantil, fraudes al utilizar ardid o engaño para afectar patrimonialmente a otra persona y así también los delitos de plagio en el caso de derechos de autor, dando origen a una pluralidad de ofensas sociales que son penalmente reconocidas pero dentro del ámbito material y no inmaterial como es el ciberespacio, por lo tanto el bien jurídico tutelado de los delitos informáticos puede considerarse pluriofensivo.

2.7. Los sujetos del delito

El Código Penal establece en su título quinto Capítulo I, la participación en el delito, y determina el grado de responsabilidad según el tiempo, modo y forma en que se participó en un hecho delictivo dentro de sus Artículos 35 al 40, describiendo a los responsables penalmente del delito siendo los denominados como: autores y los cómplices. De las faltas sólo son responsables los autores. Respecto a los autores establece que son:

a) Quienes tomen parte directa en la ejecución de los actos propios del delito.

b) Quienes fuercen o induzcan directamente a otro a ejecutarlo.

c) Quienes cooperan a la realización del delito, ya sea en su preparación o en su ejecución, con un acto sin el cual no se hubiere podido cometer.

d) Quienes habiéndose concertado con otro u otros para la ejecución de un delito, están presentes en el momento de su consumación.

En relación a los cómplices dispone que sean las personas con el siguiente comportamiento:

a) Quienes animaren o alentaren a otro en su resolución de cometer el delito.

b) Quienes prometieren su ayuda o cooperación para después de cometido el delito.

c) Quienes proporcionaren informes o suministraren medios adecuados para realizar el delito.

d) Quienes sirvieron de enlace o actuaren como intermediarios entre los partícipes para obtener la concurrencia de éstos en el delito.

También determina la responsabilidad de personas jurídicas siendo los directores, gerentes, ejecutivos, representantes, administradores, funcionarios o empleados de ellas. Otro aspecto que aborda es la participación en la comisión de hechos delictivos donde se concentra una muchedumbre de personas.

"En el caso de los delitos que atentan contra los programas de ordenador, tienden a tener un alto grado de conocimiento y recursos en el área de informática y TIC en general, en virtud que estos delitos no pueden ser cometidos por cualquier persona. Siendo las más comunes: Hacker, Cracker, Pirata informático...", dentro de las actividades delictivas que realizan es violar niveles de seguridad o la utilización de programas para poder o plataformas virtuales para lograr su cometido. "El Hacker: Este término proviene del uso del vocablo del idioma inglés hack que traducido significa cortar, tajar, hachazo. La acción de cortar los niveles de seguridad de un sistema informático se denomina hacking. Al sujeto responsable se le llama hacker. (...) Dentro de los actos realizados por este autor del delito informático se encuentra la intrusión simple, daño electrónico simple, intrusión agravada por la finalidad." [6]

"El primero denominado Intrusión Simple (hacking simple), es la acción consistente en el acceso no autorizado a un equipo informático ajeno una página web propiedad de un tercero, por cualquier medio, cuando el sujeto activo no produjere con ella ningún daño o fuere motivado por fines que puedan considerarse incluidos en otro tipo penal más

[6] **Ibíd.,** Pág. 379

grave, como tampoco produjere algún detrimento en derechos intelectuales del sujeto pasivo. // Este nivel de ilícito lo realiza el hacker, en los otros niveles se ha utilizado el término cracker." (...) Otro de los sujetos que participan en los delitos informáticos es el Cracker este: "...término proviene del vocablo inglés crack que traducido significa romperse, restallido, grieta..."[7], o romper

"En este caso se encuentran los otros niveles descritos anteriormente. El segundo es el Daño Electrónico Simple (cracking), que es la acción en la cual el sujeto activo, luego de introducirse de forma no autorizada en equipo electrónico o página web ajena, produce algún detrimento patrimonial mediante el menoscabo de la integridad física o lógica de cualquier de ellos, sin más motivo que la producción misma del daño. El tercer nivel denominado Intrusión agravada por la finalidad (Hacking económico o agravado) se define como la acción consistente en el acceso no autorizado a un equipo informático ajeno o una página web de propiedad de un tercero, por cualquier medio, cuando el sujeto activo lo hiciere a fin de obtener un beneficio económico de cualquier otro tipo para sí o un tercero. Otro sujeto del delito informático se encuentra los piratas informáticos, las acciones cometidas por ellos están ligados a los delitos de propiedad intelectual y son definido como: "...quien adopta por negocio la reproducción, apropiación o acapararían y distribución, con fines lucrativos, y a gran escala, de distintos medios y contenidos (software, videos, música) de los que no posee licencia o permiso de su autor, generalmente haciendo uso de un ordenador".[8]

[7] **Ibíd.**, Pág. 379
[8] **Ibíd.**, Pág. 380

"...por la influencia que tienen en el ambiente informático las grandes empresas de computación, en especial las titulares de los programas de ordenador más comerciales, se acuño el concepto pirata informático..." // "Los términos descritos anteriormente se utilizan para el sujeto que ejecuta la acción de forma directa, pero es importante establecer que pueden existir otra clase de responsables como el autor intelectual. El ejemplo surge cuando un sujeto que no tiene el conocimiento en informática encarga a un hacker para cometer el hecho ilícito". [9]

Los anteriores son considerados como los sujetos activos en la comisión de los delitos informativos, tanto autores como cómplices, ahora el sujeto pasivo en la comisión de un hecho ilícito si es una persona individual se denomina víctima o agraviada, si esta afecta a un grupo de personas o bien es un peligro para un grupo de personas el agraviado es la sociedad, también las personas jurídicas pueden ser víctimas de estos delitos, principalmente instituciones financieras, como bancos, financieras, aseguradores, casas emisoras de tarjetas de crédito y débito etc., también proveedores de servicios electrónicos, (internet, software, creación de páginas web, etc.), ya que toda su información se encuentra automatizada y muchas veces en el ciberespacio y su poca o nula seguridad les ha permitido ser vulnerables, otras

En relación al Estado también este se puede considerar como sujeto pasivo de los delitos informáticos, ya que toda la información ya la tiene sistematizada y puede ser objeto de hackeo, principalmente la administración tributaria, porque alteran sus programas para conseguir beneficios tributarios.

---

[9] **Ibíd.**, Pág. 380

2.8. Clases de delitos informáticos

La clasificación que a continuación se describirá es según el bien jurídico afectado, iniciando con un la argumentación siguiente: "Al definir los delitos informáticos se hacía referencia a acciones antijurídicas con una finalidad que podría ser el ataque, daño o acceso no autorizado a un aparato o sistema de computadoras o sus programas, o bien se sirve de éstas como medio operativo para realizar actos ilícitos; además de acuerdo a la real afectación al bien jurídico tutelado estos pueden ser dirigidos a vulnerar el patrimonio, propiedad intelectual o bien la privacidad o indemnidad de las personas. Estas reflexiones sirven de base para proponer por parte del autor (Noriega Salazar), la siguiente clasificación de los delitos informáticos, distinguiéndose entonces dos tipos a saber: // a) Delitos Informáticos contra el patrimonio y la propiedad intelectual. b) Delitos Informáticos que atentan contra la privacidad, la intimidad, la libertad o indemnidad sexual".[10]

"Los delitos contra bienes informáticos (TIC) y los delitos cometidos por medio de las Tecnologías de la información y la comunicación son aquellos que atentan contra bienes creados por la Informática y las Tecnologías de la información y la comunicación; en sentido amplio se consideran a los delitos informáticos los cometidos contra los bienes de origen informático así como aquellos en los que se haga uso indebido de los sistemas de información y que se encuentran regulados en otros capítulos del Código Penal e inclusive algunos que no están regulados pero que

[10] Noriega Salazar. **Op. Cit.,** Pág. 22

pueden ser considerados delito. (spam, fraude informático, subastas ilícitas, publicaciones obscenas en línea)".[11]

La clasificación de los delitos informáticos se atenderá en una breve reseña de lo propuesto por el autor Hans Aarón Noriega Salazar en su libro Delitos informáticos, determinando las clases de acuerdo al bien jurídico tutelado, donde describe que pueden ser vulnerados el patrimonio, la propiedad intelectual o bien la privacidad o la indemnidad de las personas, clasificándolos de la siguiente manera:

a) Delitos Informáticos contra el patrimonio y la propiedad intelectual.

b) Delitos Informáticos que atentan contra la privacidad, la intimidad, la libertad o indemnidad sexual.

Los delitos informáticos contra el patrimonio y la propiedad intelectual dan una lista, pero, haciendo la aseveración que no es limitativa ya que pueden existir muchos más delitos que afecten estos bienes jurídicos tutelados, siendo los siguientes:

a) La copia ilegal de software, películas y música

b) Defraudaciones a través de publicidad engañosa

c) Fraudes cometidos por medio del acceso y manipulación a sistemas informáticos bancarios o financieros.

[11] Barrios Osorio. **Op. Cit.**, Pág. 378

d) Sabotaje a sistemas informáticos,

e) Uso no autorizado de sistemas informáticos ajenos

f) Espionaje informático

g) Falsificación de documentos por medio de la computadora.

Con relación a la segunda división de delitos informáticos los que atentan contra la privacidad y la intimidad de las personas y la libertad o indemnidad sexual, les una el sujeto activo (autor y cómplices) ponen en peligro la vida privada d las personas, las conductas que se presentan en estos delitos son:

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

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

c) Pornografía infantil a través de Internet; que implica la grabación y distribución por medio de la red de imágenes de contenido sexual de niños, niñas o adolescentes. Constituye lamentablemente esta conducta una de las de mayor grado de expansión en la actualidad. No obstante, las condenas que cada vez son más

severas y numerosas la tendencia es que este tipo de delitos crezca. De igual manera la aparición de nuevas tecnologías (como la encriptación de datos por ejemplo), dificultan la persecución penal de estos ilícitos."[12]

2.9. Delitos informáticos en la legislación penal guatemalteca

Debido a que la legislación guatemalteca no estaba preparada para el advenimiento de la sistematización de la sociedad, es decir la introducción de nuevas tecnologías en el territorio, también no contaba con los tipos penales que regularan los nuevos comportamientos delictivos que se cometen en el ciberespacio, fue necesario que el Congreso de la República reformara el Código Penal, para introducir ciertos tipos penales a través del Decreto número 33-96 del Congreso de la República de Guatemala el 21 de junio del año 1996, aunque esta lista es limitada en virtud de la creciente influencia que la internet tiene cada día en la actividad humana, se describirá como una referencia legal a conductas ya legisladas.

Dentro de los considerandos de la ley y una de las razones de su creación establece: Que los avances de la tecnología obligan al Estado a legislar en bien de la población de derechos de autor en materia informática tipos delictivos que nuestra legislación no ha desarrollado. En ese sentido en materia de delitos informáticos se regulan los tipos penales que quedaran adicionados bajos los Artículos 274 "A" al 274 "G", siendo los siguientes:

a) Destrucción de registros informáticos

[12] Noriega Salazar, Hans Aarón, **Delitos Informáticos**. Pág. 24

b) Alteración de programa

c) Reproducción de

d) Instrucciones o programas de Computación

e) Registros Prohibidos.

f) Manipulación de Información

g) Uso de Información

h) Programas Destructivos

Estas conductas delictivas solo se encuentran adicionadas en el Código Penal, pero existen otras conductas para que puedan ser realizadas se necesita uno de los elementos materiales de los delitos informáticos que es el hardware o el equipo de cómputo, los delitos son los siguientes:

a) Violación a Derechos de Autor, (Artículo 274 del Código Penal).

b) Violación a los Derechos de Propiedad Industrial, (Artículo 275 del Código Penal).

c) Pánico Financiero contenido, (Artículo 342 "B" del Código Penal).

d) Ingreso a espectáculos y distribución de material pornográfico a personas menores de edad contenida, (Artículo 189 del Código Penal).

e) Violación a la intimidad sexual, (Artículo 190 del Código Penal).

f) Producción de pornografía de personas menores de edad, (Artículo 194 del Código Penal).

g) Comercialización o difusión de pornografía de personas menores de edad, (Artículo 195 Bis).

h) Posesión de material pornográfico de personas menores de edad, (Artículo 195 ter).

i) Comercialización de Datos Personales ilícito penal (Ley de Acceso a la Información Pública, Artículo 64).

j) Alteración fraudulenta contenido (Artículo 275 Bis del Código Penal).

2.10. Instrumentos internacionales sobre delitos informáticos

La extraterritorialidad de la comisión de hechos delictivos en el ciberespacio ha propiciado la preocupación de distintas entidades de Carácter internacionales quienes a través del análisis y la investigación han logrado crear instrumentos jurídicos y documentos para apoyar a los países parte para la creación adecuada a las nuevas formas de comisión de delitos basadas en la utilización de las nuevas tecnologías. Las entidades que han dispuesto al respecto es la Unión Europea, Naciones Unidas y la Organización de Estados Americanos.

2.10.1. Unión Europea (UE)

Los convenios internacionales suscritos que regulan los delitos informáticos en la Unión Europea son los siguientes son:

a) Convenio No.108 del Consejo de Europa

b) Decisión marco 2005/222/JAI del Consejo de Europa

2.10.2. Naciones Unidas (ONU)

La Organización de las Naciones Unidas y la prevención del delito informático también ha realizado diversos instrumentos de carácter internacional para establecer parámetros legales y los nuevos tipos penales informáticos, realizando lo siguiente:

a) Undécimo Congreso de Naciones Unidas para la prevención del delito y la justicia penal

b) Convención de Palermo

c) Declaración de Viena sobre la delincuencia y la justicia frente a los retos del siglo XXI

d) Resolución 57/239 sobre los elementos para la creación de una cultura mundial de seguridad cibernética

e) El manual de las Naciones Unidas para la prevención y control de delitos informáticos

f) Tratado de la organización mundial de la propiedad intelectual sobre el derecho de autor

g) Congreso de las Naciones Unidas sobre la prevención del delito y justicia penal

2.10.3. Organización de Estados Americanos (OEA)

Otra organización internacional preocupada por el avance en la ciberdelincuencia es la Organización de Estados Americanos quienes han establecido una Estrategia de la OEA sobre seguridad informática.

CAPÍTULO III

3. Las monedas criptográficas en Guatemala

En Guatemala el uso de las criptomonedas ya es un hecho, porque existen diversas empresas que lo aceptan como medio de pago dentro de plataformas virtuales, aunque sigue siendo una forma de pago transnacional digital, que no suplanta el uso de la moneda nacional, por lo tanto, se presenta como algo alegal, que a pesar de que no está legislado específicamente, tampoco está prohibido por la ley ni catalogado como un delito, como se podrá verificar más adelante.

3.1. Origen

Las criptomonedas son fórmulas matemáticas que estudian el cifrado de datos, para que puedan ser utilices en distintos aspectos de la sociedad, como la comercial, militar, política, informática, etc., por lo que se puede deducir que siempre han existido, solamente que se encontraban plasmado solo en el estudio de las matemáticas, sin embargo, la creación de la computadora permite que puedan utilizarse de forma cotidiana, ya que su uso es más útil y veloz.

Respecto al uso de la informática para el uso de la moneda digital uno de los antecedentes más próximos se da en "...los años 90 surge un movimiento denominado **cyberpunk**, el cual promueve el uso de la criptografía como mecanismo de

independencia y libertad frente al control gubernamental, gran parte de su filosofía principios se encuentran presentes en las monedas criptográficas."[13]

Este movimiento propició una serie de reuniones para que diversos pensadores puedan aportar nueva ideas libremente, contrarias a las imposiciones gubernamentales sobre el uso de la moneda oficial, además de que este tipo de investigaciones y su publicación estaba prohibido se realizó con la intención de cambiar una nueva forma de pago a través del cyberpunk, era una forma de cambiar el uso de dinero físico a dinero virtual y por lo tanto una forma de evolución social respecto al comercio, y otras transacciones económicas. "Previo a la concepción actual de monedas criptográficas han existido distintos proyectos y experimentos similares de medios privados de pago digital como: Ecash, bit gold, b-money, entre otros. [14] Estos proyectos no prosperaron por distintos factores."

En el año 2008 un grupo de programadores bajo el seudónimo de Satoshi Nakamoto, lanzo un artículo donde proponía el uso de una nueva moneda virtual, denominada Bitcoins, su colaboración se extendió con la unión a otros programadores voluntarios en el año 2010, creándose la comunidad del Bitcoin. En la actualidad es aceptado como medio de pago por muchas empresas, el protocolo que presenta es atractivo y publico a todos los usuarios dentro de su plataforma que contiene las llamadas carteras o billeteras intangibles, ya que todo es de forma virtual, siendo un nuevo sistema de efectivo electrónico que va en aumento por se ha propuesto otros sistemas monetarios

[13] Ramírez Monzón, Darío Alejandro, **Las monedas criptográficas en Guatemala**, (Análisis técnico y jurídico). Pág. 23
[14] Franco, Pedro. **Understanding Bitcoin. Cryptography, Engineering and Economics**. Pág. 161.

virtuales que han sido aceptadas y están cobrando relevancia al igual que el Bitcoin como son: Etherium (ETH), Binance Coin (BNB), Cardano (ADA), Tether (USDT), Polkadot (DOT), Ripple (XRP) y Uniswap (UNI).

3.2. Naturaleza jurídica

Para conocer la naturaleza u origen de las criptomonedas en especial dentro de la legislación guatemalteca, es necesario exponer quiénes y cómo funciona el sistema monetario en el territorio, es así que se le ha atribuido al Banco de Guatemala, entre otras funciones, es el órgano autónomo que tiene el monopolio de emisión de la moneda nacional, el quetzal, por designación de la Constitución Política de la República de Guatemala (Artículo 132) y demás leyes ordinarias. (Artículo 2 Ley Monetaria, Artículo 4 Ley Orgánica del Banco de Guatemala).

La Ley Monetaria en el Artículo tercero Circulación ilegal advierte de las consecuencias penales para toda aquella persona que haga circular monedas u otros objetos con el fin de que sirvan como moneda nacional. Es decir que las criptomonedas no forman parte de la circulación legal, por lo que su uso sería un delito, pero para poder ser parte de este tipo penal las monedas digitales deben suplantar a la nacional, algo que no ocurre, sino que son alternativas para uso digital exclusivamente

Encuadrar en el artículo tercero de la Ley Monetaria tiene una consecuencia jurídica, el delito de emisión y circulación de moneda, previsto en el Artículo 319 del Código Penal, el cual sanciona a las personas que emitan ilegítimamente piezas monetarias o las

hagan circular dentro del territorio de la república o emitan o pongan en circulación otros objetos con el fin de que sirvan como moneda. Sin embargo, el Artículo 320 del Código Penal desarrolla lo que se considera como moneda para la ley penal guatemalteca y en ninguno de esos supuestos encuadran las criptomonedas. Por lo que legalmente, de momento, no puede considerarse a las criptomonedas como monedas dentro del territorio nacional y su circulación y minería no cumplen con todos los supuestos del tipo penal.

El origen de las criptomonedas según la legislación actual dentro de Guatemala y también dentro de los Estados Unidos de América, aunque su uso se encuentra en el comercio electrónico, ya es utilizado por muchas empresas en ese medio, la legislación no le ha dado un título como moneda oficial de ningún país, es el caso de USA donde es considerado un título valor frente al Estado, sin embargo en Guatemala su naturaleza jurídica o su ubicación dentro de la legislación todavía se encuentra en una laguna legal, en virtud de que las leyes no proporcionan una base para considerarla monedas, pero tampoco como un título valor, por lo tanto la tutela estatal es inexistente.

Respecto al análisis de la moneda oficial física la Constitución Política de la República de Guatemala en su Artículo 171 (b) faculta al Congreso de la República a fijar las características de la moneda con opinión de la Junta Monetaria, sin embargo, estas peculiaridades son aplicadas al dinero físico y no virtual, o al menos esto no está muy claro. "...La teoría económica identifica al dinero por medio de tres funciones

específicas: almacenamiento de valor, medio de intercambio, unidad de cuenta. En este sentido muchos consideran que las criptomonedas cumplen perfectamente estas tres funciones; otros, en el caso de bitcoin, cuestionan la función de almacenamiento de valor, principalmente por su excesiva volatilidad. El Banco Central Inglés argumenta: Las monedas digitales cumplen las funciones del dinero sólo hasta cierto punto, y sólo para un número reducido de personas".[15] Por lo que su existencia es indudable en el mundo digital, pero no en el físico.

Para darles una validez legal dentro del territorio, las criptomonedas pueden ubicarse como bienes incorpóreos porque son objetos de apropiación, dentro de la legislación guatemalteca, también atendiendo a la clasificación por su comportamiento o forma de actuar, (Artículo 442 del Código Civil), otra disposición acorde a su naturaleza es por su uso actual por las empresas puede considerarse que no están excluidas del comercio y circulan de un lugar a otro según los regulado por el Artículo 443, 451 del Decreto Ley 106 del Jefe de Gobierno. En virtud de lo anterior la Ley del Mercado de Valores y Mercancías establece en el Artículo 2, literal b: Mercancías: Son mercancías todos aquellos bienes que no estén excluidos del comercio por su naturaleza o por disposición de la ley.

Aunque la anterior ubicación legal de las criptomonedas no es especifica sino general siempre queda el vacío legal para darle un fundamento legal más riguroso y poco confuso. También se puede observar que alrededor del mundo este tipo de monedas

[15]http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3digitalcurrenciesbitcoin2.Pdf, (Consultado el 12 de octubre de 2020)

no son consideradas valores dinerarios, sino como comodines o materias primas, esto postulado por la Comisión para el Comercio de Futuros de Mercancías (CFTC48 por sus siglas en inglés), sugiriendo que el territorio estadounidense se aleja de clasificar a bitcoin y similares como monedas y los asocia más a una mercancía.

Otros problemas para ubicar las criptomonedas dentro de la legislación son las siguientes:

a) Argumentos que consideran a las criptomonedas como títulos de crédito, que es un bien aceptado por el Código de Comercio de Guatemala, sin embargo, la misma ley las percibe como bienes muebles y no incorpóreos como son las monedas o billeteras virtuales, dejando nuevamente por un lado una base legal sólida, que necesitan para ser aceptadas en el país.

b) Son consideradas como divisas, porque este sistema monetario no es concebido por un sistema nacional monetario, sino que viene del extranjero, el problema se presenta porque las divisas son monedas extranjeras de otros países, con un sistema legal para crearlas, pero las criptomonedas son transnacionales, no tienen nacionalidad y por lo tanto no son divisas. Aunque esto se solucionaría creando una banca central para darle un origen geográfico, que es lo que se está proponiendo actualmente.

Determinar el origen jurídico y la base legal de las criptomonedas en Guatemala puede acercarse si se hace de forma integrativa, pero siempre quedan cabos sueltos, que no

permite establecer su naturaleza jurídica exacta, por lo que las reformas a la ley para su integración es la forma de darle la seguridad y validez jurídica que necesita para actuar libremente en el territorio.

3.3. Terminología

La etimología adecuada de una moneda virtual es criptografía matemática, ya que fue a través del uso de esta disciplina que permitió su creación, sin embargo, son denominadas de diferentes formas, como monedas virtuales, digitales, divisas, dinero en la red, efectivo virtual, etc. También por sus protocolos o sistemas de intercambio son llamadas de diferente manera Bitcoin, Ethereum, Ripple, IOTA, Litecoin etc.

Actualmente no se ha determinado un nombre o terminología consolidada y global sobre las criptomonedas, ya que han sido diversas agrupaciones en todo el mundo de programadores que han creado sus propios sistemas de pago a tras del dinero digital, por lo que establecer el uso oficial de una sola moneda es deber de la creación de acuerdos internacionales entre Estados para su agrupación y consolidación en una banca central. Sin embargo y derivado de los usos y costumbres digitales, la palabra moneda es la más utilizada, en relación a estos medios privados de pago.

3.4. Definiciones

Las criptomonedas son entendidas por la Autoridad Bancaria Europea como monedas virtuales: "...una representación digital de valor que no son emitidas por un banco central o una autoridad pública, ni necesariamente unidas a una moneda fiduciaria,

pero son aceptadas por personas físicas o jurídicas como medios de pago y se pueden transferir, almacenar o negociar electrónicamente."[16]

3.5. Características

Las criptomonedas o monedas digitales a diferencia de la moneda de curso legal, tiene peculiaridades que las diferencian de cualquier título valor o moneda de cambio, sus características más comunes son:

a) **Es un activo digital:** Aunque no pertenece a ningún país, ni a una banca central, sigue siendo un medio de pago aceptado por muchas empresas, distribuido en una gran cantidad de ordenadores que le dan la validez como activo.

b) **Es intangible:** su origen es a través de datos matemáticos por lo que su intangibilidad es por excelencia, ya que solo existe de manera virtual.

c) **Es creación de una ecuación matemática criptográfica:** Esta forma de pago y sus sistemas esta basa en fórmulas matemáticas financieras y contables.

d) **Son de naturaleza transnacional**: Las criptomonedas al no depender de ningún organismo nacional no tienen nacionalidad, ni tampoco dependen de una banca central internacional, por lo tanto, no existe una sede física que controle su funcionamiento.

[16]https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf, (Consultado el 12 de octubre de 2020)

3.6. Los usos de las criptomonedas

El uso es bastante extenso, bitcoin –por ser la moneda con mayor valor y popularidad– es la más utilizada prácticamente para cualquier servicio financiero, entre los usos más comunes se encuentran:

a) Medio de pago.

b) Almacenamiento de valor.

c) Especulación e inversión.

d) Trabajos en línea.

e) Envío de remesas.

3.7. Estafas comunes con Bitcoin y criptomonedas

El criptomundo ha sido tierra bastante fértil para toda clase de estafas, dado que hace falta mucha educación sobre diversos temas, y la posibilidad de lucrar a costa de los usuarios es bastante grande. Esto llegó al punto en que muchas personas llegaron a considerar (o incluso aún consideran) a bitcoin y a las criptomonedas como estafas, sin saber diferenciar entre iniciativas inescrupulosas y proyectos legítimos. Si bien las criptomonedas son utilizadas en su mayoría de forma legal, también se han convertido en atractivos tesoros para los criminales, quienes resultan bastante creativos a la hora de tender toda clase de trampas a los dueños desprevenidos. Las estafas más

comunes, tomando en cuenta que la estafa es un tipo de engaño y los malwares y hackers pertenecen a otra categoría.[17]

a) ICO fraudulentas: proyecto para recaudar fondos mediante la creación de un nuevo token preparado para ser vendido al precio del mercado, cuyo valor se respaldará en el futuro con el valor del proyecto en cuestión, cuando este sea lanzado. Las estafas se dan cuando nunca se concretan los proyectos.

b) Intercambios P2P: Se trata del simple intercambio de criptomonedas directamente entre las partes involucradas, sin la ayuda de algún intermediario de confianza, como una casa de cambio. En las redes sociales y chats abundan los anuncios de intercambio, que ofrecen comprar o vender criptomonedas con diferentes métodos de pago. Algunos pueden ser legítimos, pero otros solicitarán que envíes primero los fondos y desaparecerán con ellos.

c) Cloud Mining: "Este es un método en donde alguna empresa ofrece contratos o acciones a clientes interesados en obtener ganancias con la minería (creación) de criptomonedas sin tener que preocuparse por comprar y mantener los equipos necesarios, dado que la empresa se hará cargo de ello. A cambio de estos contratos, el usuario puede obtener ciertas ganancias de modo regular, sin mantener los equipos: de ahí Cloud Mining (minería en la nube). No se trata por sí mismo de una estafa, pues existen compañías que trabajan en Cloud Mining de

[17] https://www.criptonoticias.com/criptopedia/estafas-comunes-bitcoin-criptomonedas/, (Consultado el 12 de octubre de 2020)

forma legítima. Sin embargo, resulta muy sencillo para otros engañar a los usuarios para comprar estos contratos, ofreciendo ganancias irreales y supuestamente garantizadas, cuando ni siquiera poseen los equipos necesarios para minar."[18]

d) Regalos que comúnmente dan en redes sociales, muchas veces nunca los dan siendo un fraude.

e) Esquemas pump and dump: La táctica consiste en inflar artificialmente el precio de una criptomoneda muy poco conocida mediante la compra masiva coordinada y la promoción con anuncios fraudulentos. Una vez que el precio alcanza cierto nivel, se da una venta masiva para recoger ganancias, que vuelve a hacer caer el valor de la criptomoneda. De ahí su nombre: "infla y desecha.

f) Esquemas piramidales: Las ventas a través de esquemas piramidales también se daba con monedas de curso legal, este tipo de negocio obligan a las personas que para adquirir un producto deben conseguir más compradores, de esta manera tanto el comprador como el futuro vendedor no recibe ganancia alguna más que el propio producto que tiene, siendo el único que recibe la ganancia la persona que inicio la pirámide.

g) Phishing: consiste en la suplantación de identidad de una autoridad, empresa o incluso de alguna persona, con el fin de engañar a la víctima para que esta revele su información confidencial. De esta forma, el atacante podrá acceder a sus cuentas o carteras y robar los fondos.

[18] **Ibíd.**

h) Casas de cambio falsas: "aunque las casas de cambio ofrecen un servicio muy demandado, lo cierto es que son entes centralizados. Por tanto, una vez que transfieres allí tus criptomonedas, debes estar consciente de que, a partir de ese momento, la plataforma tiene la capacidad de controlar más allá de ti esos fondos. Y, si así lo quieren los administradores, nunca devolverlos. Es por ello que se deberían utilizar casas de cambio (y, en general, todo tipo de empresa) ya reguladas, o, como mínimo, con cierto tiempo operando y ampliamente conocidas. Ya existen casos de plataformas de este tipo creadas sólo con el propósito de quedarse con los fondos de los usuarios. Algunas ofrecen bonos por unirse en principio mientras que plantean tarifas ocultas, y otras se limitan a no permitir los retiros una vez se den suficientes depósitos."[19]

[19] **Ibíd**.

CAPÍTULO IV

4. Evaluar la creación de una unidad especializada en el Ministerio Público para perseguir los delitos cibernéticos como la estafa de inversión en criptomonedas

El Ministerio Público tiene como función principal, promover la persecución penal ante el órgano jurisdiccional correspondiente; además de dirigir la investigación en los delitos de acción pública, ejercer la acción civil en los casos previstos en la ley, entre otras; en tal sentido, es de suma importancia que esta institución pueda cumplir a cabalidad con sus funciones, para lo cual, cuenta con fiscalías y unidades especializadas, que permiten una persecución penal eficaz y efectiva; delimitando así el marco de investigación, tomando en cuenta el bien jurídico tutelado y como consecuencia, una mejor aplicación de la justicia.

Lo anterior permite vislumbrar la necesidad de la creación de una unidad especializada para perseguir los delitos cibernéticos como la estafa de inversión en criptomonedas.

4.1. Caso en Guatemala sobre estafas mediante criptomonedas

Uno de los casos que ha tenido relevancia dentro del territorio guatemalteco, sobre estafas mediante el uso de criptomonedas fue una casa de cambio que tenía una sede en Guatemala, denominada AirBit Club, los titulares fueron acusados de fraude y

lavado de dinero. Las ganancias se gastaron en autos lujosos, joyas y bienes raíces, en lugar de lo que se prometió, que era crear una minería y comercio de criptomonedas.

Según una publicación "...Los operadores de un esquema Ponzi mundial basado en criptomonedas han sido acusados de fraude y lavado de dinero tras una investigación de la Seguridad Nacional de los Estados Unidos." En el mismo sentido el Departamento de Justicia de los Estados Unidos, anuncio que: "...cuatro de los cinco presuntos operadores del AirBit Club, que supuestamente obtuvo decenas de millones de dólares de las víctimas, fueron arrestados y deberán comparecer ante el tribunal. El quinto fue arrestado en Panamá y está a la espera de ser extraditado a los Estados Unidos. La estafa se puso en marcha a finales de 2015 y se vendió como un club de comercialización de varios niveles en la criptoindustria. Los acusados supuestamente hicieron presentaciones fastuosas para alentar a los inversores a desprenderse de su dinero en efectivo, prometiendo rendimientos diarios garantizados de la minería y el comercio de criptodivisas."[20]

Aparentaba ser un portal en línea que mostraba "...efectivamente estas ganancias acumuladas, en realidad no había ninguna minería o criptocomercio. En su lugar, el dinero depositado se gastó en bienes de lujo y en inmuebles, y supuestamente se utilizó para financiar presentaciones aún más extravagantes para atraer a más víctimas. Ya en 2016, los socios del club que deseaban retirar sus ingresos se encontraban con excusas, retrasos y cargos ocultos, y al parecer se les decía que

[20]https://es.cointelegraph.com/news/airbit-club-ponzi-operators-charged-with-fraud-and-money-laundering, (Consultado, el 12 de octubre de 2020)

debían reclutar nuevos socios si querían recibir su dinero. Los acusados también trataron de ocultar el plan y su participación solicitando pagos de membresía en efectivo, supuestamente lavando por lo menos USD 20 millones de las ganancias a través de varios fideicomisos y cuentas bancarias, y eliminando de Internet la información negativa sobre la estafa. Como informó Cointelegraph el mes pasado, un miembro de otra de las primeras estafas Ponzi basadas en criptomonedas, que obtuvo USD 722 millones, se declaró culpable de los cargos de fraude electrónico y venta de valores no registrados."[21]

Este caso demuestra que los delitos cibernéticos o cometidos dentro del ciberespacio ya son un hecho en Guatemala y que muchas figuras delictivas, no son tipos penal dentro de la legislación criminal en el territorio, y por lo tanto la incapacidad de erradicar, perseguir y sancionar este tipo de conductas se ha vuelto imposible, ya que la tecnología y sus avances tanto buenos como malos, rebasan los pronósticos legislativos en la creación de tipos penales.

4.2. Convenio de Budapest y su relación con el problema planteado

La ciber delincuencia ha avanzado de la mano de los avances tecnológicos y ha sido objeto de preocupación de muchas entidades gubernamentales alrededor del mundo, asimismo se han sumado entidades internacionales para crear estrategias que puedan ayudar a combatir los delitos cometidos dentro de la internet, un ejemplo de ello es el Convenio de Budapest Convenio sobre la ciber delincuencia, del 23 de noviembre del

[21] Ibid.

año 2001. Dentro del preámbulo del Convenido de Budapest, las disposiciones relacionadas al tema son las siguientes:

a) La promoción de hacer conciencia sobre los profundos cambios provocados por la digitalización, la convergencia y la globalización continuas de las redes informáticas.

b) Determinación de la necesidad de aplicar, con carácter prioritario, una política penal común con objeto de proteger a la sociedad frente a la ciber delincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional;

c) El riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes;

d) Establecimiento de la necesidad de cooperación entre los Estados y el sector privado en la lucha contra la ciber delincuencia, así como la necesidad de proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de información;

e) Estimación de la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal;

f) Determinación de que el convenio es necesario para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos,

garantizando la tipificación como delito de dichos actos, tal como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar eficazmente contra dicho delitos, facilitando su detección investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones materiales que permitan una cooperación internacional rápida y fiable;

g) Ejecutar la garantía del debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales consagrados en el Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derecho civiles y Políticos de la Naciones Unidas (1966) y otros tratados internacionales aplicables en materia de derechos humanos, que reafirman el derecho a defender la propia opinión sin interferencia, el derecho a la libertad de expresión, incluida la libertad de buscar, obtener y comunicar información e ideas de toda índole, sin consideración de fronteras, así como el respeto de la vida privada;

También se determina dentro del Convenio que es un complemento de otros convenios para incrementar la eficacia de las investigaciones y procedimiento penales relativos a los delitos relacionados con sistemas y datos informáticos, así como permitir la obtención de prueba electrónica de los delitos.

La implementación del Convenido está determinada a nuevas formas de ciber delitos; y complementando otros convenios internacionales relacionados, asimismo; la plataforma donde se realiza la comisión de los delitos y los actores del mismo, para ello establecieron en el Artículo uno las definiciones siguientes:

a) Sistemas informáticos: se entenderá 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;

b) Datos informáticos: se entenderá toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluidos los programas diseñados para que un sistema informático ejecute una función.

c) Proveedor de servicios se entenderá: i. toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático, y ii. Cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo;

d) Datos relativos al tráfico: se entenderá todos los datos relativos a una comunicación realizada por medio de un sistema informático, generados por este último en tanto que elemento de la cadena de comunicación, y que indiquen el origen, el destino, la ruta, la hora, la fecha, el tamaño y la duración de la comunicación o el tipo de servicio subyacente.

Respecto a los tipos penales relacionados con los delitos cometidos a través de uso de portales que fomente el financiamiento con criptomonedas, el Convenio de Budapest establece en los Artículos siete y ocho lo siguiente:

a) Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la introducción, alteración, borrado o supervisión deliberados e ilegítimos de datos informáticos que genera datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente. Las partes podrán exigir que exista una intención dolosa o delictiva similar que se considere que existe responsabilidad penal.

b) Fraude informático. Las partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a. la introducción, alteración, borrado o supresión de datos informáticos; b. cualquier interferencia en el funcionamiento de un sistema informático. Con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

En el Artículo 14 del Convenio establece el ámbito de aplicación de las disposiciones de procedimiento, principalmente la legislación interna para poder crear una cooperación internacional en la persecución y al efecto disponen lo siguiente:

a) Cada parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para establecer la implementación del convenio a los efectos de investigación o de procedimiento penales específicos.

b) Cada parte aplicará el convenio en los siguientes casos: i. delitos previstos en aplicación de los artículos 2 a 11 del Convenio; ii. cualquier otro delito cometido por medio de un sistema informático; y iv. a la obtención de pruebas electrónicas de cualquier delito.

Los comportamientos dañosos delictivos que se producen dentro del internet y por la interacción internacional en la comisión de los mismos el Convenio determina en su Sección tres, Artículo 22, la Jurisdicción de la aplicación del mismo, donde cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción, cuando el delito se hay cometido:

a) En su territorio; o

b) A bordo de un buque que enarbole su pabellón; o

c) A bordo de una aeronave matriculada según sus leyes; o

d) Por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún estado tiene competencia territorial respecto del mismo.

Las partes podrán reservarse el derecho a no aplicar, o a aplicar sólo en determinados caso o condiciones, las normas sobre jurisdicción. Cada Estado adoptará las medidas que resulten necesarias para afirmarlo respecto de cualquier delito mencionado en el Convenio cuando el presunto autor del mismo se halle en su territorio y no pueda ser extraditado a otra Parte por razón únicamente de su nacionalidad, previa demanda de

extradición, también no excluye ninguna jurisdicción penal ejercida de conformidad con su derecho interno. En el caso de que varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado, los interesados celebrarán consultas cuando ello sea oportuno, con el fin de decidir qué jurisdicción es más adecuada para entablar la acción penal.

Dentro del Convenio también establece un tema de gran importancia para el problema planteado y es la cooperación internacional para la persecución y erradicación de los delitos relacionados, estableciendo como principios generales en la sección uno del Capítulo tres, titulo uno, Artículo 23 lo siguiente: Las Partes cooperarán entre sí en la mayor medida posible, en aplicación de los instrumentos internacionales pertinentes sobre cooperación internacional en materia penal, de los acuerdos basados en legislación uniforme o recíproca y de su propio derecho interno, a efectos de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para obtener pruebas en formato electrónico de los delitos.

Otro tema también que aborda el convenido son los principios relativos a la extradición, (Artículo 24 del Convenido) y principios generales a la asistencia mutua, respecto a este el Artículo 25 del presente instrumento establece:

a) Las partes se presentarán toda la ayuda mutua posible a efectos de las investigaciones o de los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o con el fin de obtener pruebas en formato electrónico de un delito.

b) Cada parte adoptará asimismo las medidas legislativas y de otro tipo que resulten necesarias para cumplir con las obligaciones establecidas en el Convenio.

c) Cada parte podrá, en caso de urgencia, formular una solicitud de asistencia mutua, o realizar las comunicaciones relativas a la misma a través de medios de comunicación rápidos, como el fax o el correo electrónico, siempre que esos medios ofrezcan niveles suficientes de seguridad y de autenticación (incluido el criptado, en caso necesario), con confirmación oficial posterior si el Estado requerido así lo exige. El Estado requerido aceptará la solicitud y responderá a la misma por cualquiera de esos medios rápidos de comunicación.

d) Salvo otra disposición relativa, la asistencia mutua estará sujeta a las condiciones establecidas en el derecho interno de la parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos sobre la base de cuales la Parte requerida pueda rechazar la cooperación. La parte requerida no deberá ejercer su derecho a rehusar la asistencia mutua únicamente porque la solicitud se refiera a un delito que dicha parte considera de carácter fiscal.

e) Cuando, de conformidad con los dispuesto en el presente capítulo, la parte requerida esté autorizada a condicionar la asistencia mutua a la existencia de doble tipificación penal, se considerará que dicha condición se satisface si el acto que constituye delito, para el que se solicita la asistencia mutua, está tipificado como tal en su derecho internó, independientemente de que dicho derecho interno incluya o no el delito en las misma categoría a lo denomine o no con la misma terminología que la parte requirente.

Basado en los principios generales de cooperación mutua, el Convenio realiza una serie de procedimientos y medidas para su implementación, dentro del título 4, en la sección dos títulos uno al tres, dentro de disposiciones específicas estableciendo lo siguiente:

a) Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables.

b) Asistencia mutua en materia de medidas provisionales: i. Conservación rápida de datos informáticos almacenados, ii. Revelación rápida de datos conservados, (Artículos 29 y 30 del Convenio).

c) Asistencia mutua en relación con los poderes de investigación: i. Asistencia mutua en relación con el acceso a datos almacenados. ii. Acceso transfronterizo a datos almacenado, con consentimiento o cuando sean accesible al público. iii. Asistencia mutua para la obtención en tiempo real de datos relativos al tráfico. iv. Asistencia mutua en relación con la interceptación de datos relativos al contenido, (Artículos 31 al 34 del Convenio).

d) Red 24/7

Respecto a las anteriores medidas la Red 24/7, es una de las alternativas que más utilidad puede tener el Estado de Guatemala, para coadyuvar al Ministerio Publico en la localización física de las personas que estén cometiendo hechos ilícitos en el ciberespacio, y principalmente los de carácter económico que utilizan plataformas

virtuales con apariencia legitima, que solamente expertos y equipos utilizados en otros Estados pueden detectar con mayor facilidad.

En relación a lo anterior el Artículo 25 del Convenio establece que cada Parte designará un punto de contacto localizable las 24 horas del día, siete días a la semana, con el fin de garantizar una asistencia inmediata para investigaciones relativas a delitos vinculados a sistemas y datos informáticos, o para obtener las pruebas en formato electrónico de un delito. Esta asistencia comprenderá toda acción que facilite las medidas que figuran a continuación, o su aplicación directa si lo permite el derecho y la práctica internos:

a) Asesoramiento técnico;

b) Conservación de datos, de conformidad con lo establecido en el Convenio; y

c) Obtención de pruebas, suministros de información de carácter jurídicos y localización de sospechosos.

El punto de contacto de una Parte dispondrá de los medios para comunicarse con el punto de contacto de otra Parte siguiendo un procedimiento acelerado. Si el punto de contacto designado por una Parte no depende de la autoridad o autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, dicho punto de contacto se asegurará de poder actuar coordinadamente con esta o estas autoridades por medio de un procedimiento acelerado. Cada parte garantizará la disponibilidad de personal formado y equipado con objeto de facilitar el funcionamiento en la red.

Es importante hacer mención de este convenio, ya que tiene una serie de disposiciones y recomendaciones de cooperación internacional que dentro de ellas se encuentre la Red 24/7, que provee a todas los Estados miembros un monitoreo permanente de información sobre ciber delitos, localización y finalmente extradición de quienes se encuentren culpables, por lo tanto es imprescindible que el Estado de Guatemala, determine un marco de cooperación para la implementación del Convenio de Budapest que permita la persecución y erradicación de los delitos cometidos con el uso de criptomonedas,

4.3. Propuesta de creación de una unidad especializada en el Ministerio Público para perseguir los delitos cibernéticos como la estafa de inversión en criptomonedas

En los títulos anteriores se demostró que la inclusión de la tecnología dentro de las actividades diarias de la sociedad, su inclusión a ella ha provocado que también la actividad delictiva este tomando un rumbo hacia la comisión de hechos criminales, dentro del ciberespacio, la velocidad en la que incrementa los hechos criminales, dejan atrás los tipos penales establecidos en la legislación y especialmente en Guatemala, que si bien es cierto ya hay delitos de carácter informático, los delitos con criptomonedas no encuadran en los supuestos ya legislado, por lo tanto normarlo y crear un ente institucional que dependa del ministerio Público para su persecución, sanción y erradicación es fundamental.

Con relación a la creación de una unidad especializada contra delitos cometidos mediante el uso de criptomonedas que dependa del Ministerio Público se propone que se realice observando las siguientes bases:

a) Por ser la jefe del Ministerio Público según lo establecido por la Ley Orgánica de dicha institución, según las funciones concedidas por la normativa citada, quien determine las políticas y decisiones que considere convenientes para el buen funcionamiento de la institución, por lo que es la encargada de crear la unidad especializada contra delitos cometidos mediante el uso de criptomonedas, a través de un Acuerdo.

b) Debe tener una coordinación con fiscalías y otras entidades del Ministerio Público. La unidad especializada contra delitos cometidos mediante el uso de criptomonedas, coadyuvara a la investigación de los delitos cometidos dentro del ciberespacio para la averiguación de la verdad, en la materia que le corresponde que es la tecnológica.

c) Coordinación con otras entidades del Gobierno. La unidad especializada contra delitos cometidos mediante el uso de criptomonedas, debe tener relación con otras entidades del Estado, principalmente con el Instituto Nacional de Ciencias Forenses, (INACIF), para obtener apoyo con las dependencias de dicha entidad y unir esfuerzos.

d) Coordinación con la Red 24/7. Atendiendo a lo establecido en el Convenio de Budapest la Red 24/7 es una alternativa útil que el Estado Guatemala puede obtener siendo parte de este instrumento internacional, debido a que creando una unidad especializada contra delitos cometidos mediante el uso de criptomonedas, no solo se cubra el territorio nacional, sino que la investigación sobrepase el país, buscando información a través de esta red y que permita una localización física más efectiva de quienes cometen hechos ilícitos alrededor del mundo; asimismo, tener oportunidad de detectar plataforma virtuales con apariencia legitima que solamente el personal especializado lo puede lograr.

e) Integración. La unidad especializada contra delitos cometidos mediante el uso de criptomonedas, puede estar integrada con: Un jefe de la unidad, quien es el encargado de la entidad, y el demás personal técnico y administrativo de apoyo que pueda requerirse, según el caso.

f) Organización. La organización estará a cargo de la Dirección de Investigaciones Criminalísticas, por ser el ente superior y dependiente, por regla general es quien debe organizar a la unidad especializada contra delitos cometidos mediante el uso de criptomonedas.

g) Otras entidades que tiene relación para poder crear unidades en el Ministerio Público son: La Jefatura Administrativa, a través de la Dirección de Recursos Humanos, Dirección Administrativa, Dirección Financiera y Dirección de Análisis y

Planificación quienes realizan la implementación de las decisiones tomadas mediante Acuerdos del Jefe del Ministerio Público.

h) Apoyo de las fiscalías a la unidad especializada contra delitos cometidos mediante el uso de criptomonedas, las fiscalías también pueden ser parte de la implementación de la unidad a través de darles apoyo que sea necesario con la finalidad de facilitarles el buen funcionamiento y propiciar el alcance de los niveles de eficiencia, eficacia y cobertura esperados.

CONCLUSIÓN DISCURSIVA

La creciente modalidad de pago virtual, a través de criptomonedas, ha permitido el incremento y la creación de nuevas formas fraudulentas de estafas, en detrimento económico de muchas víctimas, a través del internet; por lo que, muchas legislaciones penales están quedando atrás y no pueden juzgar estos ilícitos penales, como sucedió en Guatemala al extraditar a Estados Unidos a los imputados de estafas por medio del uso de criptomonedas; ya que dentro de la legislación no existen los tipos penales que encuadren con esta conducta, para poder llevar a cabo dentro del territorio, el juicio.

El Ministerio Público no cuenta con una unidad especializada para perseguir los delitos cibernéticos, como la estafa de inversión en criptomonedas; además, no existe en la legislación, una norma jurídica que regule, defina, permita, prohíba o sancione el uso de monedas criptográficas.

En virtud de lo anterior, es necesario que el Jefe del Ministerio Público, mediante acuerdo, cree una unidad especializada para la persecución y erradicación del delito; además de establecer un marco de cooperación que permita la implementación del Convenio de Budapest, determinando la legislación adecuada por fraudes informáticos, realizados con el uso y promoción de criptomonedas.


FACULTAD DE CIENCIAS JURIDICAS Y
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
SECRETARIA
GUATEMALA, C.A.

BIBLIOGRAFÍA

BARRIOS OSORIO, Omar Ricardo. **Derecho e informática, aspectos fundamentales**. 3ª. ed. Guatemala: Ed. Mayte, 2006.

FRANCO, Pedro. **Understanding Bitcoin. Cryptography, Engineering and Economics**.United Kingdom. Estados Unidos de America: Ed. WILEY FINANCE SERIES, 2015.

http://www.bankofengland.co.uk/publications/Documents/quarterlybulletin/2014/qb14q3 digitalcurrenciesbitcoin2. Pdf, (Consultado el 12 de octubre de 2020)

http://www.onu.org.gt/, (Consultado el 2 de julio de 2021)

http://www.rae.es/ (Consultado el 2 de julio de 2021)

https://es.cointelegraph.com/news/airbit-club-ponzi-operators-charged-with-fraud-and-money-laundering, (Consultado, el 12 de octubre de 2020)

https://www.criptonoticias.com/criptopedia/estafas-comunes-bitcoin-criptomonedas/, (Consultado el 12 de octubre de 2020)

https://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf, (Consultado el 12 de octubre de 2020)

NORIEGA SALAZAR, Han Aarón, **Delitos informáticos,** Instituto de la Defensa Pública Penal, Guatemala Ed: IDPP, 2011.

RAMÍREZ MONZÓN, Darío Alejandro, **Las monedas criptográficas en Guatemala**, (Análisis técnico y jurídico), Guatemala: Ed. Banca Central, 2016

Legislación:

Constitución Política de la República de Guatemala. Asamblea Nacional Constituyente, 1986

Código Civil y sus reformas, Decreto ley 106 del jefe de gobierno, 1963

Código de Comercio de Guatemala, Decreto 2-70 del Congreso de la República de Guatemala y sus reformas. 1970.

Código penal. Decreto 17-73 del Congreso de la República de Guatemala y sus reformas. 1973

Ley del Mercado de Valores y Mercancías. Decreto 34-96 del Congreso de la República de Guatemala. 1996.

Ley del Organismo Judicial. Decreto 2-89 del Congreso de la República de Guatemala y sus reformas 1989.

Ley Monetaria. Decreto 17-2002 del Congreso de la República de Guatemala. 2002

Ley Orgánica del Banco de Guatemala. Decreto 16-2002 del Congreso de la República de Guatemala. 2002

Reglamento para la autorización y funcionamiento de las casas de cambio, Resolución de la Junta Monetaria 131-2001. 2001.

Convenio sobre la ciberdelincuencia, Consejo de Europa, Budapest, 2001