UNIVERSIDAD GERARDO BARRIOS FACULTAD DE POSTGRADO Y EDUCACIÓN CONTINUA MAESTRÍA EN DERECHO PENAL

TEMA:

"LOS EFECTOS JURÍDICOS E INCIDENCIAS DEL DELITO DE HURTO DE IDENTIDAD EN LA LEY ESPECIAL DE DELITOS INFORMÁTICOS Y CONEXOS, EN LA ZONA ORIENTAL".

TRABAJO PARA OPTAR AL GRADO DE:

MAESTRA EN DERECHO PENAL

PRESENTADO POR:

LICDA. AMAYA COLATO JACQUELINE DEL CARMEN

LICDA. MÉNDEZ ARGUETA OSIRIS ELINOR

LICDA. ZELAYA SAGASTIZADO KAREN MAYELI

ASESOR:

Msc. VÍCTOR MANUEL RODRIGUEZ LUNA

EL SALVADOR, SAN MIGUEL, AGOSTO DE 2017.

AGRADECIMIENTOS

"Mira que te mando que te esfuerces y que seas valiente, no temas, ni desmayes que Jehová tu Dios estará contigo a donde quiera que vayas" Josué 1:9

A mi Dios, Padre, Hijo y Espíritu Santo, agradecer infinitamente por cada uno de mis logros, por cada una de sus bendiciones a mi vida.

A mi Familia, por ese apoyo incondicional en cada etapa de vida.

A mi Esposo Jim Albert Cruz Guardado, tu amor, tu apoyo, es idóneo para mí, gracias por estar a mi lado, eres el compañero perfecto para mí. Te Amo.

A mis compañeras de Tesis:

Karen Mayeli Zelaya de Romero, te quiero mucho mí Mayo, que Dios te bendiga grandemente.

Osiris Elinor Mendez Argueta, gracias por esa paciencia Osa, eso te hace especial, te quiero mucho, Dios te guie, te bendiga y acompañe siempre.

Gracias a ambas por haber emprendido este camino juntas con problemas, obstáculos, malos entendidos, pero la presencia de Dios siempre guio nuestros caminos, y gracias a Él, lo logramos.

Att. JACQUELINE DEL CARMEN AMAYA COLATO.

AGRADECIMIENTOS.

Me mostrarás la senda de la vida;
en tu presencia hay plenitud de gozo;
delicias a tu diestra para siempre.

Salmo 16:11

*A **Dios, Padre Celestial**, quien siempre me lleva de su mano y me ha dado cada logro familiar, profesional y laboral, a quien me ama y permite que cada proyecto en mi vida se realice.*

*A mis padres, **Cecilio Méndez** y **Gloria Delmi Argueta**, que siempre me apoyan en todos mis proyectos de vida, animándome y brindándome su infinito amor, celebrando conmigo cada logro como las personas más importantes que tengo.*

*A mi amada **tía Fita**, que como una madre me ha brindado soporte y amor, mi confidente y concejera, alegre de mis triunfos y cómplice de ellos.*

*A mis hermanos, **Dorian, Juan José y Tony**, adorados tormentos y cimiento de mis logros y frutos, ellos son mi inspiración y fortaleza, gracias por no fallarme nunca.*

A mis primos, que con sus palabras me dan ánimos y fuerzas, que siempre se compromete y confían en mis retos.

*A mis amigos y amigas, en especial a **Edgar Sorto** y **Hermes David**, porque han sido un apoyo fundamental durante toda la maestría, brindándonos su tiempo y compartiendo sus conocimientos sin restricciones, mis hermanos elegidos, los amo. Así mismo, a mi amigo "estrella", que ha sido más que un asesor, un maestro, compartiendo con mucha disposición su tiempo y enseñanzas, que siempre tendré presentes no solo en este proyecto, sino también, en la vida.*

*Mis compañeras de maestría y equipo de tesis, mis amigas, **Karen Mayeli** (mi gorda) y **Jacqueline Amaya** (mi chele), con quienes iniciamos este gran reto y ahora culminamos victoriosas este proyecto gracias a nuestro Creador, gracias por su apoyo, tolerancia y dedicación a este que fue nuestro proyecto.*

Licenciado Víctor Luna, asesor de tesis, por su aporte y tiempo valioso dedicado a nuestro tema de investigación.

Osiris Elinor Méndez Argueta

AGRADECIMIENTOS

Dios, tu amor y bondad no tiene fin, cada uno mis logros familiares y profesionales, son gracias a Ti, porque sin Ti nada soy y contigo todo lo puedo.

A mi madre, Masyeli del Carmen Sagastizado, por su apoyo e incondicionalidad, por su amor y compañía a lo largo de mi vida, por acompañarme en cada uno de mis retos y por ser parte fundamental para el logro de los mismos.

A mi esposo, Inmer Romero, por ser mi compañero, amigo, novio y hoy por la bendición de Dios mi esposo, que con su amor y compañía me ha dado ánimos para cumplir con este proyecto que juntos iniciamos.

A mis amigas y compañeras de tesis, Jacqueline Amaya y Osiris Elinor Méndez, quienes con su dedicación, paciencia y perseverancia fueron pilar fundamental en este proceso que iniciamos y culminamos.

A mis amigos y personas especiales, quienes sin esperar nada a cambio compartieron su conocimiento, quienes estuvieron a mi lado de forma única y especial, apoyándome y logrando que este sueño sea realidad.

A mi asesar de tesis, Licenciado Víctor Luna, por su tiempo, dedicación y por sus aportes en nuestro tema de investigación.

Karen Mayeli Zelaya Sagastizado

ÍNDICE

INTRODUCCIÓN

El Derecho está en constante cambio, es dinámico, por lo que, si la sociedad se desarrolla, el derecho también. Dicho progreso ha sido posible en gran parte por la tecnología e informática, que en el transcurso de la historia ha cambiado de generación en generación para ayudar al ser humano en sus distintas actividades como puede ir desde cuestiones laborales, estudiantiles hasta el ocio.

Es por ello que se ha visto la imperiosa necesidad de innovar, crear una nueva ciencia jurídica, de acorde a la época tecnológica, como es el derecho informático, ciencia autónoma del derecho, especializada en el tema de la informática, usos, aplicaciones e implicaciones legales. Sin embargo, no puede ser tratada de una manera aislada, pues está relacionada con las demás ciencias jurídicas como el derecho penal, derecho civil y derecho comercial.

Y específicamente en el derecho penal, en el año 2016, en El Salvador, surge como una manera de contrarrestar la parte negativa del avance tecnológico, la aprobación de la Ley Especial de Delitos Informáticos y Conexos, donde se regula el delito de Hurto de Identidad, por lo que en el proceso de esta investigación se desarrollarán los efectos jurídicos e incidencias de dicho ilícito, específicamente en la zona oriental. -

El anteproyecto se desarrolla en tres capítulos, con el siguiente contenido más relevante: Problema de investigación, este plantea la Situación Problemática que contiene la descripción de la investigación sobre el objeto en estudio, descripciones de hechos o problemas que ocurren por falta del estudio, determinando la importancia de estudiar sobre los efectos jurídicos he incidencias del delito Hurto de Identidad, como un problema jurídico social para la persecución e investigación de esta actividad. Delimitación: aquí se detallará el tiempo, espacio y la temática que se aplicará al derecho penal. Enunciado del problema, ¿En qué sentido es necesario identificar los efectos jurídicos e incidencias del delito de Hurto de Identidad en la Ley Especial de Delitos Informáticos y Conexos en la Zona Oriental?

Se visualiza que la criminalidad informática tiene un alcance mayor y su cometimiento puede llevar inmersos delitos tradicionales como la estafa, la extorsión, amenazas y el hurto, en los cuales las computadoras y los sistemas informáticos han sido utilizados como medio para el cometimiento de ilícitos; entonces, con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

Al mismo tiempo vemos como las instituciones encargadas de la investigación y el proceso sancionatorio, carecen de herramientas modernas para hacer una práctica efectiva del combate a la impunidad de este ilícito, además del creciente índice que cometimiento de estos, no siempre para obtener un lucro económico o de beneficio propio, sino también, para ocasionar daños a la moral o integridad de la víctima. -

CAPITULO I

1.1 SITUACIÓN PROBLEMÁTICA.

La Identidad de la persona es una percepción material y jurídica que permite acreditar o establecer la existencia del individuo en la sociedad y que se hace a través de una serie de datos o características que de forma inequívoca permite identificar que se trata de esta. Es además un Derecho Jurídicamente relavante e inalienable y a su vez elemento importante de la personalidad. Por ello, los Estados adoptan medidas legales para reconocerla y protegerla en su uso, de esa forma, evitar fraude en las operaciones jurídicas que se realicen con ella.

De ahí, que las nuevas formas de fraude en su uso han dado inicio a una discusión jurídica de la manera en que la identidad puede ser objeto de USURPACION, SUPLANTACION o USO INDEBIDO, y los EFECTOS JURIDICOS que provoca. Ese planteamiento surge de los retos y la necesidad de dar respuestas a las nuevas tecnologías y su uso en las diferentes actividades de la vida.

Con la globalización y la llegada de la era digital en el mundo, la vulnerabilidad de sufrir un hurto o usurpación de la identidad es aun mayor y en el caso de El Salvador, la población ha adquirido una profunda y necesaria dependencia de la tecnología, derivada del uso de esta, asimismo, la facilidad que estos medios digitales permiten para obtener la información del individuo y luego hacer uso de ellos de manera fraudulenta.

Los mecanismos mas comunes que permiten la Usurpación, Suplantación o Hurto de la Identidad es a través de la red y redes sociales que amplía la posibilidad de realizar acciones encaminadas a cometer fraude o cualquier ilícito relacionado con el uso de la identidad.

La identidad surge desde el momento en que un individuo existe jurídicamente, es decir, con el nacimiento y la posterior inscripción en un registro público; es esta forma en que se da un nombre y una nacionalidad que permite identificar e individualizar al sujeto en todas sus relaciones con las demás personas. Por ello la importancia que el Estado garantice a todos sus conciudadanos el derecho a la identidad, protección y preservación

de la misma. Fijando normas de orden público, (Derecho Penal y Especial) que configura o describen las posibles acciones que atenten contra el uso fraudulento de la identidad, ejemplo de ello es la utilización de la imagen o nombre de otro, la suposición u ocultación del estado familiar, la suplantación o alteración del estado familiar, alteración de la filiación, entre otros.

Asimismo, se encuentra otro instrumento legal de carácter especial de protección como es el art. 22 de la Ley Especial de Delitos Informáticos y conexos que relaciona el Hurto de Identidad y que es sujeto de la problemática a investigar, por lo que el ámbito de aplicación de esta norma conlleva a una circunstancia especial como es en el uso de operaciones jurídica empleando o utilizando tecnologías de informática o de comunicación. En este punto en particular es menester señalar las diversas formas de fraude y las posibles consecuencias en el mundo jurídico

La red es la herramienta que se utiliza para simplificar la comunicación del individuo con el mundo y es esta cada vez mas indispensable y necesaria de utilizar en todas las actividades del individuo, muestra de ello son las múltiples operaciones bancarias móviles, transacciones y operaciones mercantiles, realización de negocios o contrato digitales nacionales o internacionales y recientemente el uso de las firmas digitales, no menos importante es la seguridad en el uso de los perfiles o cuentas personales en las redes a través de las TIC's (Tecnologías Informáticas y la Comunicación), con fines criminales con diversas intenciones ilegales como podría ser la Extorsión, Estafa, Defraudación a la Economía publica o privada.

El Uso de la TIC's aumenta el volumen y sofisticación de las amenazas y por ello también la necesidad a la protección de bienes jurídicos susceptibles de afectación y la prevención de los delitos cometidos por medio de la TIC´s.

Se perfila entonces, que el desafío de la investigación de ilícitos tecnológicos se ve agravado por la falta de herramientas jurídicas e internacionales que permitan la persecución de acciones delictivas en el uso de las TIC's.

Existen fronteras en el ciberespacio, que facilita el cometimiento de delitos informáticos a gran distancia teniendo en cuenta que todas las tecnologías informáticas o

de comunicación del mundo son un punto de entrada potencial, esto dificulta la investigación y procesamiento de estos hechos punibles. Los criminales buscan constantemente explotar vulnerabilidades para lucrarse y satisfacer sus necesidades, ya sean estas de índole económica o de perjuicio a la integridad de las personas.

Es por esta eminente amenaza, que el tema objeto de estudio lo delimitaremos en la aplicación de la Ley Especial de Delitos Informáticos y Conexos, enfocándonos particularmente en el delito de Hurto de Identidad, y sus consecuencias en el ámbito de las operaciones jurídico y económico.

Vemos que, por las características principales de los delitos informáticos, el Hurto de Identidad es difícil pero no imposibles de demostrar; ya que, en muchos casos, es complicado encontrar las pruebas, como la fuente o comprensión del ciberdelito, dificultades y respuesta jurídica. Son actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones este delito puede cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.

El delito de Hurto de Identidad en la Ley Especial de los Delitos Informáticos y Conexos, está relacionado con el contenido de los datos, de manera que perjudica de forma directa a los individuos, sea natural o jurídica, considerándose como un delito pluriofensivo, por proteger bienes jurídicos como: la identidad y confidencialidad de los datos, patrimonio, seguridad, información y propiedad.

Esta conducta punible posee características como: a) es perpetrado en torno a sistemas informáticos en donde la red tiene una relevancia limitada o secundaria para llevar a cabo la acción; b) presenta dificultades probatorias dado las limitaciones de herramientas técnicas para su comprobación; c) provoca pérdidas económicas y daños morales; d) tiende a proliferarse cada vez más.[1] Por lo que, además de las medidas que la empresa privada pueda implementar para prevenir este tipo de delitos que desfavorecen a sus clientes, es necesario también, combatir la inactividad de acudir al sistema para la restauración del derecho afectado y la impunidad del mismo en algunos casos.

En los últimos años, en el país y particularmente en la zona Oriental y a nivel nacional, se han multiplicado los sucesos en los que, especialmente por medios informáticos, se cometen fraudes económicos haciendo uso de tecnologías e información falsa en la identidad. Considerando como el crimen por excelencia del siglo XXI, con la ligera o limitada investigación, por carecer por una parte técnica pericial para detectar y descubrir los responsables de los hechos delictuosos.

Es importante destacar que la mayoría de los organismos internacionales que han abordado el tema del Hurto de Identidad, han establecido un concepto en torno al mismo, pero en lo que se han quedado cortos es, en acordar mecanismos jurídicos de carácter internacional para contrarrestar este flagelo.

Es por ello, que el tiempo actual nos desnuda una realidad y nos permite cuestionarnos la necesidad de que se revisen las diferentes legislaciones vigentes y adecuar la realidad y la necesidad, de esa forma, avanzar en el tema del HURTO DE IDENTIDAD, y sus diferentes manifestaciones a través de ese mundo tan inmenso e inimaginable como lo es, la red.

La independencia de una rama del derecho no quiere decir que se aísle de la ciencia jurídica, sino que aborde los problemas con instituciones propias, correspondiente a la materia que se investiga, en este caso la informática, relacionada específicamente a los delitos tecnológicos (Hurto de Identidad).

Por lo tanto, la indagación permitirá proporcionar una herramienta práctica a las instituciones involucradas en la investigación, así como a profesionales y estudiantes de derecho, órgano judicial y población en general, para que el delito de Hurto de Identidad, sea denunciado, investigado, procesado y condenado de manera efectiva y justa.

1.2 DELIMITACIÓN DEL PROYECTO

a) ESPACIO.

La indagación de los casos en los que ha seguido un proceso penal referido al delito de Hurto de Identidad, se delimitara en los departamentos de la zona oriental, en virtud que esto permitirá estudiar con mayor profundidad y precisión la temática planteada, de igual manera, por ser accesible para la investigación jurídico dogmática, requerida para confrontar la realidad con la doctrina, tomando como datos específicos de la Unidad Especializada de la Fiscalía General de la República de Patrimonio Privado y Propiedad Intelectual, Procuraduría General de la República y la Policía Nacional Civil, así como los Juzgados, Tribunales de primera instancia y segunda instancia.

Las anteriores entidades nos facilitaran el desglose sistemático y objetivo de la aplicación de la Ley Especial contra los Delitos Informáticos y Conexos, específicamente en el delito de Hurto de Identidad, para obtener datos básicos y estadísticos en el desarrollo de la indagación, y por la facilidad de traslado para efectuar la misma. No se debe de olvidar que la presente investigación por el carácter dogmático, jurídico y jurisprudencial que presenta, permitirá dar un realce en la obtención de información, por esta razón se ejecutara en un inicio espacio geográfico determinado y delimitado anteriormente mencionado, también por los datos que se pueden obtener de muestras de los Juzgados de Paz, de Instrucción y Sentencia útiles para el desarrollo de la temática.

B) TIEMPO.

Para realizar la presente investigación, es importante determinar el tiempo que comprenderá, porque estos proporcionan variables esenciales para la observación de forma y contenido del tema. El tiempo de la investigación, se delimitará desde enero de dos mil diecisiete, a julio del año en referencia, temporalidad que de acuerdo a la efectividad de ejecución de investigación para el desarrollo y aplicación del tema en análisis se pretende abarcar, por ser un periodo donde los objetivos planteados serán cumplidos, asimismo por criterios de actualidad y factibilidad para el equipo investigador.

c) TEMÁTICA:

La investigación estará delimitada por un análisis jurídico, dogmático y jurisprudencial, en el que se pretenderá acotar las diversas opiniones de juristas, tratadistas, para unificar posturas únicamente sobre la interpretación del tipo penal del Hurto de Identidad de la Ley Especial de Delitos Informáticos y Conexos

1.3 ENUNCIADOS DEL PROBLEMA.

1.3.1 ENUNCIADOS GENERAL:

- ¿En qué sentido es necesario identificar los efectos jurídicos e incidencias del delito de Hurto de Identidad en la Ley Especial de Delitos Informáticos y Conexos en la zona oriental?

1.3.2 ENUNCIADOS ESPECÍFICOS:

- ¿Cuál es la interpretación adecuada del delito de Hurto de Identidad, desde la perspectiva dogmática jurídica en las diversas modalidades de la conducta típica?
- ¿Cuál es la importancia de estudiar las debilidades que presenta el sistema jurídico en el tipo del delito de Hurto de Identidad?
- ¿Para quienes servirían las recomendaciones técnicas-teóricas que surjan de la investigación del delito de Hurto de Identidad en su aplicación práctica?

1.4 JUSTIFICACIÓN.

Los delitos informáticos están presentes en la actualidad en cualquier parte del mundo en la que se tenga acceso a un medio virtual y electrónico, esto conlleva a que la información que publicamos en redes sociales, perfiles, correos entre otros puede llegar a ser vulnerada. Este tipo de acceso a la privacidad de una persona puede afectar no solo su vida financiera sino también su vida personal.

La utilización de dispositivos electrónicos es cada vez es más frecuente, debido al avance tecnológico y la necesidad de comunicación de las personas por medio de formas más agiles y eficientes, enviar información es algo inevitable sobre todo en aquellos casos en que las distancias son más largas. Cualquier tipo de información que se envié por medios electrónicos puede ser alcanzada por un ciberdelincuente.

A nivel internacional se han ido creando leyes y mecanismos para la investigación, persecución y sanción de los delitos informáticos, también se han creado dependencias en las diferentes instituciones de seguridad que buscan ponerle freno a las acciones delictivas cometida por este tipo de personas.

La información que se suministra en las redes sociales es de gran valor para aquellas personas que se toman el tiempo de investigar la vida de los demás, ello con la intención de atentar con la identidad digital, sin darnos cuenta nosotros mismos proveemos información valiosa no solo de nuestra vida y actividades sino también de quienes nos rodean. Desafortunadamente, cuando una persona se da cuenta de que sus datos han sido vulnerados es demasiado tarde.

La criminalidad informática tiene un alcance mayor y su cometimiento puede llevar inmersos delitos tradicionales, como la estafa, la extorsión, amenazas y el hurto, en los cuales las computadoras y los sistemas informáticos han sido utilizados como medio para el cometimiento de ilícitos; Con el desarrollo de la programación y de Internet, los delitos informáticos se han vuelto más frecuentes y sofisticados.

En razón de lo anterior es necesaria la aplicación de leyes que tienen por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la

prevención y sanción de los delitos cometidos en las variedades existentes contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías.

Una misma acción dirigida contra un sistema informático puede aparejar la violación de varias leyes penales, es así que tenemos que por medio del delito de Hurto de Identidad, luego de obtener los datos personales de un individuo, se procede a realizar todo tipo de operaciones para provecho del hechor, fingiendo ser la persona a la que se extrajo su información sensible, y logrando con ello realizar otras acciones punibles, lo que hace necesario que se realice una investigación encaminada a la detección, sanción y erradicación de dicha figura delictiva.

1.5 OBJETIVOS.

1.5.1 GENERAL:

- Identificar los efectos jurídicos e incidencias del delito de Hurto de Identidad en la Ley Especial de Delitos Informáticos y Conexos en la zona oriental.

1.5.2 ESPECÍFICOS:

- Determinar las prácticas de las conductas delictivas realizadas por medio del delito de Hurto de Identidad.

- Analizar las debilidades que presenta el sistema jurídico en el tipo de delito de Hurto de Identidad.

- Formular y proponer recomendaciones técnicas-teóricas que faciliten la investigación del delito de Hurto de Identidad y su aplicación práctica.

CAPITULO II

2. METODOLOGÍA DE LA INVESTIGACIÓN

2.1. TIPO DE ESTUDIO.

TEÓRICO DESCRIPTIVO:

Se hará uso de este tipo de estudio con el objetivo de conocer las situaciones, prácticas y modos predominantes mediante la descripción exacta de las actividades y procesos, que se relacionen con las posturas sobre la correcta interpretación de tipo penal de Hurto de Identidad, donde se puntualizara el registro, análisis e interpretación de naturaleza actual, composición y dominantes posturas de los diversos autores, basados sobre realidades de hechos y sus características fundamentales atinentes al tema de investigación.

PRÁCTICO ANALÍTICO

Este tipo de estudio admite la utilización de métodos de validez, existiendo una relación entre la teoría y la práctica, se vincula el proceso y las instituciones intervinientes.

Con el análisis de los documentos y fuentes que tratan el problema de estudio, se fijaran parámetros mediante los cuales el Hurto de Identidad regulado en la Ley Especial contra los Delitos Informáticos y Conexos, debe estar regida, principalmente con los elementos que conforman la teoría dogmática jurídica del delito, fundada bajo los presupuestos mínimos que exige la normativa legal.

2.2. MÉTODO.

MÉTODO HISTÓRICO.

Permite desarrollar el origen, evolución, datos actuales, y consecuencias del objeto de estudio, logrando una búsqueda crítica de la realidad y la verdad. Se utilizan técnicas de investigación documental; que parte de la utilización de libros, artículos, revistas,

folletos, boletines, conferencias, leyes, tratados internacionales entre otros, relacionados con el tema de investigación en su devenir histórico.

Se emplea la síntesis, Mario Tamayo la define como: "*El método que procede de lo simple a lo complejo, de las causas a los efectos, de la parte al todo*".[2] La necesidad para auxiliarse de este instrumento permite llegar a la formulación de consideraciones finales que representan la esencia del problema que se investiga en la evolución legal.

MÉTODO ANALÍTICO.

Además, se hace uso del referido método el cual consiste en adquirir un conocimiento auto correctivo y progresivo, con el que se pretende descomponer o desintegrar gran cantidad de intuición en partes, para lograr hacer una estructuración de todos los elementos importantes determinantes en la investigación. A través del análisis se determinará la incidencia y efectos jurídicos del delito de Hurto de Identidad regulado en la Ley Especial contra los delitos informáticos y conexos.

2.3. POBLACIÓN, MUESTRA Y UNIDAD DE ANÁLISIS.

Toda investigación consta de dos fases trascendentales, ellas son: la teoría y la práctica, la primera tiene como finalidad la recopilación de datos, para ello es necesario la construcción de cuadros estadísticos y gráficos, que demuestre lo que expresan los postulados dogmáticos y doctrinarios en contraste con la realidad; y eso solo es posible con la identificación y conceptualización de los siguientes elementos:

POBLACIÓN.

La población está constituida por 50 personas, integradas en las diversas instituciones implicadas dentro de un proceso penal en el que se conozca el delito de Hurto de Identidad, como Magistrados, Jueces, Fiscales, Defensores Públicos; por lo que

[2] Mario Tamayo. (2004). *Diccionario de la investigación científica*, 2da Edición, editorial LIMUSA, México, pág. 135.

se realizarán visitas a Juzgados de Paz, de Instrucción y Sentencia, Fiscalía General de la República y Procuraduría General de la República.

MUESTRA.

Delimitada la población, se procederá a la obtención de una muestra representativa, dada las características del estudio, se ha decidido trabajar con la totalidad de la población, debido a que una de las características de la población es el ser relativamente pequeña, y en atención a la circunstancia de que se desea obtener un dato más apegado a la realidad, eliminando así el margen de error.

UNIDADES DE ANÁLISIS.

a) Juzgados de Paz de las cabeceras de los departamentos de San Miguel, Usulután, Morazán y La Unión, el delito de Hurto de Identidad y su iniciación con la correspondiente apertura de investigación, es el Juez quien autoriza esa fase, ello da lugar a que se encuentre relacionado directamente con la autorización de dicha institución jurídica.

b) Juzgados de Instrucción de las cabeceras de los departamentos de San Miguel, Usulután, Morazán y La Unión, comprende la audiencia preliminar y la etapa de instrucción, debido a ello es que este juzgado se constituye en un rubro necesario para la recolección de información sobre el instituto jurídico en estudio.

c) Los Fiscales, por ser ellos quienes ejercen la acción penal, asignados a la Unidad de Patrimonio Privado y Propiedad Intelectual de la Fiscalía General de la República, a través de requerimiento y dictámenes de acusación, al Juez correspondiente, debidamente fundamentada, para el esclarecimiento del delito de Hurto de Identidad que conocen.

d) Los Defensores Públicos, estos como garantes del derecho de defensa que tiene todo acusado, intervienen en los procesos donde se ventila el delito de Hurto de Identidad.

2.4. TÉCNICAS E INSTRUMENTOS.

Se puede llamar técnica "*a los procedimientos específicos utilizados por una ciencia determinada*[3]". Son los medios correctos de ejecutar las operaciones de interés del área que se está estudiando.

Las técnicas que se utilizan en la investigación se conforman por dos modalidades: documental y de campo, para que tenga el carácter analítico es necesario el auxilio de la diversidad de bibliografía relacionada con el tema objeto de estudio, haciendo uso de fuentes directa y mediatas que traten el problema, así como las opiniones que pueden proporcionar todos aquellos jurisconsultos que poseen un conocimiento especializado relativo al delito de Hurto de Identidad.

TÉCNICA DE INVESTIGACIÓN DOCUMENTAL O BIBLIOGRÁFICA.

Se puede realizar de forma independiente o como parte de la investigación de campo, en ambos casos, busca conocer las contribuciones durante la evolución histórica; en tal sentido se efectúa con el propósito de reunir informaciones y conocimientos previos sobre un problema para el cual se busca una respuesta sobre una hipótesis que se requiere experimentar.

En la investigación sobre los efectos jurídicos e incidencias del delito de Hurto de Identidad en la Ley Especial de Delitos Informáticos y Conexos, se ha realizado una recopilación de diversos documentos, divididos en:

Fuentes primarias: son documentos principales que sirven de guía para fundamentar la investigación, considerando los siguientes: Constitución de la República, Tratados Internacionales, Código Procesal Penal y Ley Especial de Delitos Informáticos y Conexos; Manuales de Derecho Procesal Penal, manuales de Derecho Constitucional, libros sobre derecho probatorio, etc.

[3] Santiago, Zorrilla, (214). *Metodología de la Investigación*, editorial McGraw-Hill, 5ª Edición, Madrid, España, Pág. 30.

Fuentes secundarias: son compilaciones y listados de referencia publicados en un área de conocimientos en particular, de éstas se han tomado en consideración las siguientes: Jurisprudencia internacional, legislaciones extranjeras, libros de metodología, revistas y artículos atinentes al tema de investigación.

TÉCNICAS DE INVESTIGACIÓN DE CAMPO.

Se realiza en el área de las ciencias sociales y psicológicas, algunas de sus técnicas son igualmente utilizadas para la recolección de datos complementarios en otras áreas de las ciencias; esta técnica tiene como finalidad recoger y registrar de forma ordenada los datos relativos al tema escogido como objeto de estudio, equivalen, por lo tanto, a instrumentos de observación controlada.

Entre las principales técnicas se destacan la entrevista, cuestionario, formulario, test, entre otros; para la presente investigación, se ha decidido hacer uso de las encuestas no estructuradas, estructuradas y semiestructuradas.

a) Encuesta no estructurada: es una forma de obtener información que se diferencia de la conversación ocasional, porque ésta es provocada con una finalidad de información precisa a través del intercambio de opiniones, presentándose difícilmente la cuantificación, está será dirigida a especialistas del tema, por lo que el aporte será cualitativo.

La pregunta puede ser modificada y adaptarse a las situaciones y características particulares del sujeto, el investigador puede seguir otras pautas al entrevistar.

b) Encuesta estructurada: es aquella que se hace de acuerdo con la estructura de la investigación y puede ser de orden rígido o flexible, las rígidamente estructuradas son de orden formal y presentan un estilo idéntico del planteamiento de las preguntas y en igual orden a cada uno de los participantes, son flexibles cuando conservan la estructura de la pregunta, pero su formulación obedece a las características del participante.

Se realiza a los sujetos que intervienen en el proceso investigativo, como fiscales, defensores públicos y particulares.

2.5. ETAPAS DE LA INVESTIGACIÓN.

La investigación se dividirá en cuatro etapas relativamente ordenadas: Investigación bibliográfica, investigación de campo, procesamiento de la información y el nivel descriptivo.

Investigación Bibliográfica: se recopilará información de libros en las diferentes bibliotecas del país donde se identifique que existe material bibliográfico con contenido referente al tema objeto de estudio, así como en la página de la Corte Suprema de Justicia, para verificar si existe jurisprudencia sobre el tema en investigación. De igual forma se visitarán páginas web que contengan datos sobre el delito de Hurto de Identidad.

Investigación de Campo: una vez clasificada la información se realizarán los contactos con personas especialistas o instituciones implicadas que conozcan sobre el delito de Hurto de Identidad, como magistrados, jueces, fiscales, defensores públicos o entidades del Estado que se encuentren en la zona oriental, dentro del territorio salvadoreño.

Procesamiento de la Información Bibliográfica y de Campo: obtenida esta se realizará el análisis de la misma durante el proceso de la investigación.

La investigación se realiza en sentido amplio, en los niveles descriptivos y práctico analítico.

En cuanto al **teórico descriptivo**, tendrá como finalidad conocer las situaciones prácticas y modos predominantes, mediante la descripción exacta de las actividades y procesos que se relaciona con la postura del tipo penal de Hurto de Identidad.

Nivel **práctico analítico**, con el análisis de los documentos y fuentes que tratan al problema de estudio se fijaran parámetros de los elementos que conforman la teoría dogmática jurídica del delito.

2.6. PROCEDIMIENTO DE ANÁLISIS E INTERPRETACIÓN DE RESULTADOS.

La información de la investigación se procesará de las estadísticas de las encuestas estructuradas, no estructuradas y semiestructuradas, a través de la tabulación.-

PRINCIPALES UNIDADES DE ANÁLISIS EN LA INVESTIGACIÓN.

UNIDAD DE ANÁLISIS	POBLACIÓN	MUESTRA	INSTRUMENTO
Especialista en derecho penal	2	2	Encuesta No Estructurada
Magistrados	2	2	Encuesta No Estructurada
Jueces	8	8	Encuesta Semi-Estructurada
Fiscales	10	10	Encuesta Semi-Estructurada
Defensores Públicos	10	10	Encuesta Estructurada
Defensores Privados	10	10	Encuesta Estructurada
División de la Unidad de Especializada de Delitos Informáticos de la Policía Nacional Civil.	8	8	Encuesta Estructurada
Total	50	50	

CAPITULO III
3. MARCO TEÓRICO

3.1. ANTECEDENTES HISTÓRICOS.

El avance que ha tenido la tecnología es de notable importancia para el derecho, ya que con el surgimiento de la Informática Jurídica [4] que se ha desarrollado intensamente en la cultura mundial, se han abarcado todos los ámbitos de las relaciones sociales y jurídicas, debiéndose enfrentar a grandes cambios en muchos aspectos que dependen cada día más de una adecuada evolución, entre los que podemos mencionar son el ámbito legal, las relaciones comerciales y la administración pública.

Robo de identidad y también llamado en algunas legislaciones, Hurto de Identidad, una de las actividades ilícitas que ha trascendido de manera considerable en algunos países, es el llamado robo de identidad o mejor conocido como identity theft [5](voz inglesa). Apropiación ilegal de identidad. Este fenómeno delictivo afecta en algunos casos de manera inmediata a las víctimas que lo padecen, y en otros casos las repercusiones se manifiestan a largo plazo, ejemplo de ello, cuando una persona utiliza la identidad de otra para realizar una solicitud de crédito, procedimiento que es desconocido por la víctima, pero a mediano plazo ésta empieza a recibir notificaciones de la deuda existente por un crédito que jamás solicitó, o en casos extremos le es comunicada que es perseguida por la justicia.

La parte afectada en esta problemática sin lugar a duda es la víctima, quien pierde de manera específica, su identidad legal, su estabilidad económica, en casos extremos su libertad, y principalmente se encuentra ante un inevitable daño moral, donde su prestigio o su imagen se ven completamente dañadas ante los ojos de la sociedad o de la justicia.

---

[4] Sergio, Matute. (2012), *Los Sistemas de Información, La Informática Jurídica, y el sistema UNAN JURE*. Segunda Edición, Editorial UNAM Jurídica, México, Pág. 107.

[5] Verónica Fernández. (2014). *La protección y seguridad de la persona en internet: Aspectos sociales y jurídicos*. Primera edición, Editorial Reus S.A., Madrid, España. Pág. 52.

Vemos para ello un ejemplo de Puerto Rico, relacionada al delito de Hurto de Identidad por medio de la apropiación ilegal de identidad: “La apropiación ilegal de identidad ocurre cuando se utiliza la información de una persona con la intención de cometer, ayudar o proporcionar cualquier actividad ilícita que constituya una violación de ley federal o delito grave bajo cualquier ley estatal. El robo de identidad se ha convertido en uno de los delitos más populares de los últimos años. Desde el 2004 se contempló en el Código Penal en el Art. 216 como Apropiación Ilegal de Identidad. Este delito afecta a las víctimas no solo financieramente sino emocionalmente, pues se tiene que probar que las acciones y transacciones fueron cometidas por otra persona.

La Apropiación Ilegal de Identidad es un crimen que afecta, especialmente a miles de menores anualmente y la cifra reportada refleja índices en aumento. Según estadísticas de la Federal Trade Comission (FTC) en el año 2005, el 5% de los casos reportados eran de personas menores de 18 años. En el 2006, se reflejó un aumento de un 2% adicional para elevarlo a 7%. Según las principales casas de crédito, el número puede ser mayor ya que este tipo de crimen usualmente no es descubierto hasta que las víctimas son adultos y tratan de establecer crédito por lo que, este tipo de fraude en menores puede pasar sin ser detectado por muchos años”.[6]

Los antecedentes de los delitos informáticos van a la par del desarrollo de las tecnologías de la información; con el adelanto de la tecnología, la sociedad se ha visto en un panorama de avance y desarrollo en todas sus áreas; trágicamente, la delincuencia también se ha beneficiado de esto. Entre los beneficios que ofrece el uso de redes de comunicación a los delincuentes, se encuentran: la capacidad de cometer delitos desde cualquier parte del planeta, velocidad, gran cantidad de víctimas potenciales y anonimato, entre otros.

Uno de los primeros y más importantes ataques en la historia de Internet se remonta a CREEPER en 1971, escrito por el ingeniero Bob Thomas, es considerado el primer virus informático que afecto a una computadora, el cual mostraba un mensaje en los equipos infectados, y si bien, no causaba daño alguno, fue la base para el desarrollo

[6] Asamblea Legislativa, Senado de Puerto Rico (2009), *Informe Negativo, sobre el P. del S, Segunda Sesión Ordinaria 16ta*. 4 de noviembre de 2009. Pág. 2.

de ataques posteriores con pérdidas multimillonarias, como se menciona en el sitio web de la INTERPOL "se estima que en 2007 y 2008 la ciberdelincuencia tuvo un coste a escala mundial de unos 8.000 millones de USD[7]".

Para dar prioridad a la demanda de la ciudadanía que ha sido víctima de robo de identidad y por la magnitud de éste, así como la amenaza que representa para la población, algunos países han puesto su atención y conciben de manera específica a esta conducta como "un crimen federal que ocurre cuando la identificación de la persona es utilizada o transferida por otra persona, para actividades ilegales".

Entre las actividades más destacadas por este delito se encuentra las siguientes:

- Quejas relacionadas con el robo de identidad.
- Fraude con Tarjetas de Pago.
- Servicios no Autorizados de Servicios Públicos o Teléfono.
- Fraude Bancario.
- Préstamos Fraudulentos.
- Documentos o Beneficios Gubernamentales.

Estafas de robo de identidad más utilizadas[8]:

- Sorteos falsos u obras de beneficencia falsificadas.
- Trabajos en el hogar que ofrecen ganar dinero fácil.
- Tarjeta de pago, protección de crédito u ofertas de reparación de créditos falsos.
- Ofertas de viajes a tarifa reducida u ofertas con descuento en revistas.
- Estafas de Becas.

Otra forma de delinquir realizada a nivel mundial, derivada de la obtención de datos personales para actividades ilegales es, el delito informático, definido como "Cualquier comportamiento criminal en que la computadora u otros periféricos o

[7] Loredo González, Jesús Alberto. (2013). *Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo.* Editorial FCFM-UANL, Facultad de Ciencias Físico Matemáticas Universidad Autónoma de Nuevo León San Nicolás de los Garza, Nuevo León, México. Pág. 45.

[8] Marco, Gercke. (2013). *Manual sobre los delitos relacionados con la identidad*. Oficina de las Naciones Unidas contra la Droga y el Delito. Naciones Unidas, Nueva York, 2013. Pág. 07.

dispositivos informáticos, estén involucrados como material, objeto o símbolo para perpetuar un fraude, engaño, o delito informático tipificado[9]". Por su parte, Estados Unidos, Canadá, y la mayoría de los países europeos, han determinado que existen tres tipos de comportamiento ilícito relacionado con los delitos informáticos:

- Acceso no autorizado.
- Actos dañinos o circulación de material dañino.
- Intercepción no autorizada.

Estos tres tipos fueron tipificados y penalizados por los sistemas legales de aquellas naciones, pero desde el punto de vista criminológico algunos autores clasifican a los delitos informáticos desde dos variantes:

- Como instrumento o medio.
- Como fin u objetivo.

Estas dos apreciaciones se entienden de la siguiente manera:

Como instrumento o medio: se tiene como manifiesto aquellas conductas criminógenas que utilizan la tecnología para utilizarla como artificio para ejecutar actividades ilícitas.

Como fin u objetivo: En esta etapa las conductas criminógenas rechazan la presencia de la computadora o programa entendido como entidad física, mientras que por su parte otros conciben a esta como una clasificación sui géneris, como los llamados -delitos electrónicos-, mismos que se dividen en tres categorías[10]:

[9] Delfino,López (2013). *La suplantación de identidad de tipo físico, informático y de telecomunicaciones como nueva manifestación de las conductas antisociales*. Revista Colectivo Arcion, visión criminológica-criminalística, Puebla, México. Pág. 07.

[10] Julio, Téllez (2003). *Derecho Informático*. 3ª edición, Editorial McGraw Hill Serie Jurídica, México. Pág. 285.

1. Individuos que a beneficio utilizan la tecnología electrónica como un método, es decir, esta vía es un medio cuyo objetivo es llegar a consumar una actividad ilícita.

2. De aquellas personas que a través de la innovación de la tecnología electrónica usan la computadora como herramienta principal para cometer sus fechorías.

3. Los que se valen del avance tecnológico para cometer un solo fin: dañar el medio electrónico.

La seguridad internacional se ha visto amenazada por intrusos del internet, que se introducen en los sistemas para robar información confidencial y vulnerar al país, como el tan famoso gusano de internet proyectado en Estados Unidos de América, en el año de 1988, por Robert Morris Jr., mismo que fue detenido y sancionado gracias a la existencia del acta fraude y abuso informático que circulaba durante esa época.

Los delitos informáticos han atormentado la economía de diferentes países, como el caso de Estados Unidos de América, en el que su pérdida económica alcanza los 10,000 millones de dólares, esta información es brindada por las compañías de seguros contratadas por estas potencias mundiales, mismas que registran que es tan grande el daño y perjuicio económico que se propone crear grupos exclusivos de investigadores especializados en delitos informáticos.

Tan solo el Federal Bureau of Investigation (FBI). Oficina Federal de Investigaciones, ha atendido tan solo el 90% de los delitos informáticos perpetrados vía internet en los Estados Unidos de América. [11]

Las redes de comunicación hoy en día "era de la comunicación"[12], se han vuelto una necesidad, y no un lujo, como se creía en épocas pasadas, ahora acceder a internet

[11] Juan Manuel Pérez. (2013). *El criminólogo-criminalista ante el fenómeno delictivo*. Año 1 Número1, Enero-Marzo 2013. Colectivo Arcion. Puebla, México. Pág. 11.

[12] Algunos autores se han referido al proceso de desarrollo de la influencia la tecnología informática como la segunda revolución industrial, que sus efectos pueden ser aún más transformadores que los de la industrial del

significa fuente de empleo, comunicación, transacciones, desarrollo, publicidad, imagen, entre otras cosas.

Una de las herramientas indispensables en ésta época es la llamada red de comunicación mejor conocida como internet, el cual no estaba diseñado para las inferencias criminales de los últimos años[13], los protocolos con los que se cuenta no se encuentran protegidos, por ello es que en la actualidad, se puede observar ataques contra la seguridad por parte de hackers.

En la actualidad la extensión de la informática y de las redes, como Internet, ha alcanzado la vida diaria de las personas y organizaciones, y la importancia que tiene su progreso para el desarrollo del país, ha hecho que los peligros que sufre la información almacenada en los diversos sistemas informáticos, crezcan y se diversifiquen, debiéndose tomar medidas legales que se han adoptado, pero hasta el momento han resultado insuficientes.

Vemos como otros países del mundo principalmente en Europa, Estados Unidos y unos pocos países de América del Sur, se ha creado la imperiosa necesidad de introducir a sus sistemas normativos convenios internacionales para el combate más efectivo a estos delitos tecnológicos, por lo que firman el Convenio sobre ciberdelincuencia, también conocido como el Convenio de Budapest sobre ciberdelincuencia o simplemente como Convenio Budapest, es el primer tratado internacional que busca hacer frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes nacionales, la mejora de las técnicas de investigación y el aumento de la cooperación entre las naciones. Fue elaborado por el Consejo de Europa en Estrasburgo, con la participación activa de los Estados observadores de Canadá, Japón y China.

El Convenio y su Informe Explicativo fueron aprobados por el Comité de Ministros del Consejo de Europa en su 109ª reunión, el 8 de noviembre de 2001. El 23 de noviembre de 2001, se abrió a la firma en Budapest y entró en vigor el 1 de julio de

---

siglo XIX. Ulrich, Sieber, (1992). "*Documentación Para Aproximación Al Delito Informático*", publicado en Delincuencia, Editorial. PPU, Barcelona, España. Pág. 65.

[13] Delfino, López. (2013). *Óp. Cit.* Pág. 08.

2004. A partir del 28 de octubre de 2010, 30 estados firmaron, ratificaron y se adhirieron a la Convención, mientras que otros 16 estados firmaron la Convención, pero no la ratificaron.

El 1 de marzo de 2006, el Protocolo Adicional a la Convención sobre Cibercrimen entró en vigor. Los Estados que han ratificado el Protocolo Adicional son necesarios para penalizar la difusión de propaganda racista y xenófoba a través de los sistemas informáticos, así como de las amenazas racistas y xenófobas e insultos.

EN EL SALVADOR

Para referirnos a la historia del delito de Hurto de Identidad en nuestro país, antes de la entrada en vigencia de la Ley Especial de Delitos Informáticos y Conexos, nos hacemos la siguiente interrogante ¿cómo era procesada y sancionada la acción de suplantar o apoderarse de la identidad de una persona natural o jurídica por medio de las Tecnologías de la Información y la Comunicación?

Para obtener una respuesta apegada al fin de la normativa penal, nos referimos a la propia Ley que en uno de los considerandos, especifica que la realización de esta acción ante el perjuicio de un bien jurídico quedaba en la impunidad.

La que literalmente dice: "Que esta diversidad de actividades delincuenciales que pueden cometerse a través de las Tecnologías de la Información y la Comunicación, no se encuentran suficientemente reguladas en nuestra normativa penal vigente, generándose una impunidad para quienes cometen estos tipos de delitos; en consecuencia, resulta necesaria su tipificación y la adopción de mecanismos suficientes para facilitar su detección, investigación y sanción de estos nuevos tipos de delitos". [14]

La ley castiga con penas desde uno a seis años de prisión el acceso indebido a sistemas, programas, o datos informáticos, la tenencia de equipos para vulnerar seguridad y daños. Se imponen las penas más altas, hasta 10 años de cárcel se impondrían por los delitos de estafa, fraude, espionaje informático, y hurto por medios informáticos.

[14] Asamblea Legislativa. Decreto N°260. Considerando IV. San Salvador, 26 de febrero de 2016.

Esto nos indica que antes de la tipificación del delito en estudio, no se sancionaba esa acción, pero si los ilícitos que se cometían como consecuencia o fin último de la realización del Hurto de Identidad, llamado también robo o usurpación de identidad, sin duda siempre causando perjuicio a un bien jurídico.[15]

La nueva normativa que fue aprobada con 70 votos favorables, regula los delitos de fraude informático, espionaje, estafa, pornografía, acoso sexual, Hurto de Identidad, entre otros, ilícitos que se cometan por la vía de los medios informáticos y será aplicada a cualquier persona, natural o jurídica, nacional o extranjera, por delitos que afecten bienes jurídicos del Estado, de sus habitantes o protegidos por Pactos o Tratados Internacionales ratificados por El Salvador, plantea el artículo 2 del Decreto.

El diputado Misael Mejía, del Grupo Parlamentario del FMLN y Secretario de la Comisión de Seguridad Pública y Combate a la Narcoactividad, destacó que en la Ley se incluyen sanciones por el cometimiento de delitos de acoso sexual, utilización de niños, niñas y adolescentes en pornografía y otro tipo de abusos que se comenten a través del uso de tecnologías de la información, con penas que van de 2 a 12 años de prisión.

Además, se establecen sanciones con penas de tres a cinco años a quienes suplanten o se apodere de la identidad de una persona natural o jurídica a través de tecnologías de la información, y la pena se incrementa hasta los ocho años si con esa conducta se daña, extorsiona, defrauda, injuria o amenaza para ocasionar perjuicio u obtener beneficios para sí mismo o terceros.

"Las sanciones previstas en dicha Ley, son aplicables sin perjuicio de otras responsabilidades penales, civiles o administrativas en que se incurra", así lo reza el artículo 35 de la cita normativa [16]que también dieron sus aportes a esta nueva herramienta jurídica que contribuye combatir los delitos cibernéticos en el país.

---

[15] ww.gpfmln.sv. (08 de febrero de 2016). *http://www.gpfmln.sv*. Recuperado el 22 de marzo de 2017, de http://www.gpfmln.sv/index.php/2-prensa/sesion-plenaria/1093-08021602.

[16] Asamblea.gob.sv. (18 de agosto de 2015). *http://www.asamblea.gob.sv*. Recuperado el 21 de marzo de 2017, de http://www.asamblea.gob.sv/noticias/archivo-de-noticias/retoman-estudio-de-ley-contra-delitos-informaticos.

3.2. DEFINICIÓN DE HURTO DE IDENTIDAD Y SU COMPLEJIDAD.

Desde el punto de vista del Derecho "la Identidad hace referencia a un conjunto de características, datos o informaciones que permiten individualizar a una persona".[17] En consecuencia, la atribución de una identidad permite establecer las posibles consecuencias de una conducta para su autor; la imputación de un hecho o conducta a una o varias personas determinadas mediante su identidad es el presupuesto necesario para que hacia ella o ellas se dirijan los efectos que pudieran derivarse, es decir la identidad en el ámbito jurídico tiene una significación fundamental relacional y atributiva.

En la actualidad, con el desarrollo y uso de las nuevas tecnologías de la información y de la comunicación (TIC's), han surgido determinados comportamientos de relevancia penal que podrían ser, en los supuestos más graves, merecedores de reproche penal.[18] El uso indiscriminado de las redes sociales, en cuanto que sirve de medio en muchas ocasiones para entablar relaciones personales, ha multiplicado las posibilidades de realizar conductas que afectan a la vida íntima y personal de los ciudadanos.

La potencialidad de la informática a través del empleo de las nuevas tecnologías conlleva riesgos que deben ser minimizados con respuestas adecuadas a las nuevas demandas jurídicas que requieren estas manifestaciones criminales, que propician el uso de las tecnologías de la información y de la comunicación. [19]

---

[17] Carrasco Luis, De Salvador. (2010), *Casos de suplantación de identidad detectados en denuncias tramitadas por la Agencia Española de Protección de Datos, citado por Mata y Martín, Ricardo en El robo de identidad: ¿una figura necesaria?* Ed.Arazandi-Thomson Reuters-Agencia Española de Protección de Datos-Universidad de Castilla-La Mancha. Pamplona, España, pág. 2001.

[18] Ricardo, Mata y Martin. (2010). *El robo de identidad: ¿una figura necesaria? en robo de identidad y protección de datos*. Ed.Arazandi-Thomson Reuters-Agencia Española de Protección de Datos-Universidad de Castilla-La Mancha, Pamplona, España. Pág. 200.

[19] Ibídem. Pág. 201.

El denominado “Hurto de Identidad” “Usurpación de identidad” “suplantación de Identidad” “Falsificación de la Identidad y su uso indebido” de acuerdo con investigaciones internacionales realizadas por el Consejo Económico y Social (ECOSOC) de la Organización de las Naciones Unidas, la Unión Europea y la Organización para la Cooperación y el Desarrollo Económico (OCDE)[20] es el delito de más rápido crecimiento en el mundo sin que existan acciones legislativas concretas y políticas publicas acertadas para sancionar esta conducta atípica en el plano penal.

3.2.1 DEFINICIONES GENERALES.

El Hurto de Identidad ocurre cuando una persona obtiene datos pertenecientes a otra (la victima) y se hace pasar por esta última[21]. La definición contiene dos elementos clave: El primer elemento consiste en obtener la información, y el segundo es la necesidad de hacerse pasar por la víctima. Por consiguiente, la definición no abarca el mero hecho de obtener la información, ni tampoco el de hacerse con información ajena con la intención de venderla.

La definición es bastante amplia, ya que abarca todos los actos punibles en que la identidad es el blanco o el instrumento principal, de igual forma no especifica el objeto que acoge, ni los actos delictivos, incluye varios delitos relacionados con la identidad, tales como el robo y la falsificación de identidad o la usurpación de esta.

También se ha utilizado la expresión uso indebido de la identidad [22] que tiene un significado análogo, pero no lleva implícita la presunción que determinada conducta es un delito en sí o deba ser tipificada como tal. Dado su amplio alcance, la definición no resulta apropiada para servir de base a una disposición de derecho penal, aunque es útil desde el

---

[20] Rodolfo, Romero Flores. (2016). *Las conductas vinculadas a la suplantación de identidad por medios telemáticos: una propuesta de acción legislativa*. Editorial UNAM, México, Pág. 851.

[21] Patricia Faraldo, Cabana, (2010). *Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico;* Revista de Derecho Penal y Criminología, Época, N° 3, Coruña, España, Págs. 88.

[22] Rebollo Delgado, Lucrecio, (2014) *El Derecho de la Protección de los Datos en España y Argentina, Origines y evolución reciente.* Editorial Dykinson, Madrid, España, Págs. 12.

punto de vista metodológico para tener en cuenta diversas conductas que han de examinarse al elaborar tipologías concretas y adoptar posibles medidas legislativas sobre la penalización.

Otra actividad ilegal en que la identidad es instrumento, se da cuando se constituye un fraude informático,[23] como cuando se utiliza la identidad de una persona como principal medio sin su consentimiento. Esta definición de la expresión "Hurto de Identidad" es muy similar a la anterior. Contiene dos elementos fundamentales: el objeto (la identidad) y el acto correspondiente (el fraude u otra actividad ilegal). No se dan más detalles para describir el objeto ni el acto.

Concluyendo que la expresión "Hurto de Identidad" podría ser empleada para describir el robo o la usurpación de una identidad [24] existente (o de una parte importante de la misma), con o sin consentimiento, independientemente de que la víctima esté viva o muerta.

Esta definición también contiene dos elementos: el objeto (la identidad) y el acto correspondiente (la usurpación). Comparada con otras definiciones, proporciona una descripción más detallada del objeto, aunque la definición del acto se basa en la obtención de la identidad. En consecuencia, no abarca la transferencia de información relativa a la identidad ni la utilización de dicha información.

La definición de hurto de identidad tiende a ser demasiado amplia, si se analiza la utilización de las expresiones Hurto de Identidad y falsificación de identidad en los medios de comunicación, estos van encaminadas a calificar los delitos tradicionales, como la estafa con tarjetas de crédito. Siendo esto observado por expertos de las Naciones Unidas, donde sugieren que las expresiones antes dichas se utilizarán para abarcar dichas sub categorías, como son hurto de identidad falsificación de identidad.

---

[23] María Luz, Gutiérrez F. (2011). *Notos sobre la delincuencia informática: atentados contra le información como valor económico de la empresa*. Editorial San Marcos, Lima, Perú, pág. 60.

[24] Luis Gerardo, Gabaldón, (2008) *Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico.* Editorial Sociologías, Porto Alegre, Brasil, Nº 20, pág. 164.

La expresión “delito de identidad” se utiliza generalmente para referirse a todo tipo de conductas ilícitas relacionadas con la identidad, en particular el hurto y la falsificación de identidad. El delito de identidad abarca delitos preparatorios o constitutivos como el de falsificación y de suplantación de la identidad. El problema que plantea la definición es que el uso indebido de la identidad [25] puede guardar relación con la información de identidad propiamente dicha o con otra información vinculada a esta.

Una de las principales preocupaciones relacionadas con el uso de la expresión “Hurto de Identidad” reside en que los delincuentes casi nunca sustraen el elemento tangible. Aparte de cuestiones de orden dogmático, el término hurto o robo no es preciso porque la persona cuya propiedad se sustrae suele ser la única víctima, mientras que en los casos de Hurto de Identidad, la persona cuya información se utiliza indebidamente no siempre es la única víctima[26].

Tampoco es adecuada la expresión falsificación de identidad porque la motivación de los delincuentes que se apropian de información de identidad no siempre se relaciona con la falsificación. Si bien una expresión común podría ser útil, para examinar las soluciones jurídicas se recomienda diferenciar con mayor precisión los delitos relacionados con la identidad.[27]

3.2.2 CRITERIOS PARA CONFIGURARSE EL DELITO DE HURTO DE IDENTIDAD.

La dilucidación de los delitos vinculados con la identidad contiene en general categorías con diferentes elementos que conlleva al fenómeno del Hurto de Identidad, exponiendo cierta coincidencia que puede servir para extraer criterios comunes para darse el delito.

---

[25] Lucrecio, Rebollo D. (2012). *El derecho a la protección de datos en España y Argentina orígenes y revolución vigente*. Editorial Dykinson, Madrid, España. Pág. 12.

[26] González de la Vega, Francisco, (1998). *Derecho penal mexicano, los delitos en general*. Vigésima cuarta edición. México, Editorial Porrúa. Pág. 251.

[27] Marco, Gercke. Óp. Cit. Pág. 09.

IDENTIDAD.

Se constituye como el criterio más significativo y como el primer acto preparatorio[28], como es la obtención de la información de la identidad protegida; siendo el trascendental blanco la información que se suministra en las redes sociales, siendo esta de gran valor para aquellas personas que tienen el tiempo de investigar la vida de los demás, siendo muchas veces las mismas victimas quienes suministran información valiosa, estos es debido que muy pocas personas son conscientes de la influencia que tienen los Delitos Informáticos en la actualidad y por esto no tienen mecanismos de defensa y control sobre la información que comparten a través de los medios electrónicos

A raíz de lo antes expuesto es de vital importancia decidir el alcance, de la definición de información relacionada con la identidad, ya que algunos datos digitales, como contraseñas, firmas digitales[29], nombres de cuentas e información de acceso, pueden no considerarse elementos de la identidad jurídica de una persona. Sin embargo, teniendo en cuenta el uso de ciertos datos para acceder a los servicios digitales, es necesario decidir si esa información debe incluirse en la definición.

- Los actos delictivos (que incluyen desde la obtención de la información hasta su utilización).

[28] Escamilla, Margarita Martínez. (2012). *Derecho Penal. Introducción a la Teoría Jurídica Del Delito*. Materiales para su docencia y aprendizaje. Editorial Complutense, Madrid, España. Pág. 197. La autora determina que la fase preparatoria es una fase intermedia, que no tiene por qué producirse necesariamente, entre la fase puramente interna (se ha traspasado la esfera de la simple deliberación) y la fase de ejecución material del delito. Esta fase se inicia cuando el sujeto realiza los llamados actos preparatorios.

[29] Torres Álvarez, Hernan (2005). *El sistema de Seguridad Jurídica en el Comercio Electrónico*. Primera edición, Editorial de la Pontifica Universidad Católica de Perú. Lima, Perú. Pág. 77. Al respecto la firma electrónica, según estas dos definiciones, es un término muy genérico, en el cual se diluyen las funciones de identificación y de autenticación. Por esta razón, para dotar el concepto de firma electrónica con las funciones mencionadas, debe estar complementado con la indicación de que se debe garantizar que ha sido creada por medios que estén bajo exclusivo control de una persona determinada, de manera que solo esta se encuentre vinculada a su firma.

ACTOS Y ETAPAS

En segundo lugar, es preciso establecer los actos que deberían tipificarse como delitos. La distinción entre las cuatro etapas podría ayudar a prevenir tanto carencias como superposiciones.

Etapa 1 (actos preparatorios), cuando los delitos no se ejecutan espontáneamente requieren una etapa preparatoria que con frecuencia no es un acto penalizado; la fase de ejecución se inicia cuando el autor realiza los primeros actos ejecutivos, esto es, aquellos actos que suponen un inicio de la conducta típica[30]. En relación a los delitos relacionados con la identidad, es menester decidir si los actos preparatorios, como el diseño de programas informáticos malignos o el envío de correos electrónicos de peska, deberían ser tipificados como delitos, siendo este un criterio que suscita preocupaciones por una posible penalización excesiva. Los actos relacionados con la etapa uno, podrían no tipificarse, especialmente si el sistema de derecho penal nacional no reconoce generalmente como delitos los actos preparatorios.

Etapa 2 (obtención de la información), esta etapa constituye el criterio más importante para el cometimiento del delito, siendo que la identidad es un aspecto ampliamente primordial del delito de Hurto de Identidad. Los hechores utilizan diferentes técnicas para hacerse de la información, abarcando diversos métodos y se tipifica como delito la "obtención" y la "transferencia" de información relacionada con la identidad. Bajo este argumento, es necesario tener en cuenta dos situaciones concretas.

Como primera situación, varias estafas concernidas con el Hurto de Identidad se basan en la revelación por la propia víctima al dar información sobre su identidad, gracias a la acción de mecanismos de ingeniería social [31] que se imponen a la víctima sin que esta lo advierta, por lo que al ampliarse el campo de los Delitos Informáticos, también se han creado dependencias en las diferentes instituciones de seguridad que buscan ponerle freno a las acciones delictivas cometidas por este tipo de personas.

[30] Escamilla, Margarita M. Óp. cit. Pág. 187.

[31] De Miguel, María del Rosario. (2007). *Deontología y aspectos legales de la informática: cuestiones éticas, jurídicas y técnicas básicas*. ISBN 978-84-8363-112-6, Valencia, España. Pág. 122.

La segunda situación, en que podrían observarse dificultades similares, es la obtención de información relacionada con la identidad, que pertenece al dominio público, esto conlleva a que la información que publicamos en redes sociales, perfiles, correos entre otros puede llegar a ser vulnerada. Este tipo de acceso a la privacidad de una persona puede afectar no solo su vida financiera sino también su vida personal.

Etapa 3 (proceso de transferencia), su principal característica es la transferencia de la información vinculada con la identidad ya que los hechores son individuos con una gran especialización en informática, que conocen muy bien las particularidades de la programación de sistemas computarizados, de forma tal que logran un manejo muy solvente de las herramientas necesarias para violar la seguridad de un sistema automatizado, por lo que el procesamiento de los autores de este tipo de actos es relativamente más difícil.

Los criterios que incluyen actos como la transferencia o más concretamente, la transmisión o venta de información son generalmente aplicables en estos casos. En los países cuya legislación no reconoce efectivamente delitos específicos relacionados con el Hurto de Identidad y que, por tanto, recurren a disposiciones penales tradicionales sobre el fraude y la falsificación.

Fase 4 (uso con fines delictivos). Muchos de los "delitos informáticos"[32] encuadran dentro del concepto de "delitos de cuello blanco", término introducido por primera vez por el criminólogo estadounidense[33] Edwin Sutherland en 1943. Esta categoría requiere que:

1- El sujeto activo del delito sea una persona de cierto estatus socio-económico.

2- Su comisión no pueda explicarse por falta de medios económicos, carencia de recreación, poca educación, poca inteligencia, ni por inestabilidad emocional, ya que en algunos casos la motivación del delito informático no es económica, sino

[32] Wikipedia. Delito Informático. https://es.wikipedia.org/wiki/Delito_inform%C3%A1tico (consultado el 18 de marzo de 2017).

[33] Mohrenschlager, Manfred. (1992). "*El Nuevo Derecho Penal informático en Alemania*". Delincuencia Informática. Ed. P.P.U. Colección IU RA-7). Madrid, España. Pág. 143.

que se relaciona con el deseo de ejercitar, y a veces hacer conocer a otras personas, los conocimientos o habilidades del delincuente en ese campo.

Quedando evidenciado que las motivaciones de los delincuentes que se apoderan y utilizan la información relacionada con la identidad son tan variadas como los métodos utilizados para su obtención. En general, existen dos criterios diferentes relacionados con la tipificación de los actos de esta etapa. Las formas más corrientes de utilizar la información relacionada con la identidad (por ejemplo, cometer un fraude, extorsionar etc.), ya están previstas en las disposiciones penales tradicionales, pero algunos enfoques no incluyen los actos relacionados con la etapa 4, sino, tan solo un vínculo con esos delitos en la medida en que exigen la intención de cometer el acto delictivo[34]. Otros enfoques tipifican el acto de utilizar la información relacionada con la identidad (con la intención de cometer una actividad ilegal), además, del propio delito, por lo que acceso a la privacidad de una persona puede afectar no solo su vida financiera sino también su vida personal.

- El elemento de intencionalidad (que va desde el conocimiento hasta una intención especial) .

INTENCIONALIDAD.

Uno de los métodos considerados para penalizar un acto consiste en exigir la intencionalidad[35] de cometer el hecho delictivo, el querer y conocer el acto a ejecutar; como requisito adicional de la falta de autorización de la víctima.

---

[34] Tellez Valdés, Julio (1996). "*Los Delitos informáticos. Situación en México*", Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida. Pág. 85. Conceptualiza acto delictivo en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".

[35] Aguirre Huerta, J. (1998). "*La necesidad de incluir la preterintención como forma de imputabilidad y atribuibilidad en el Código Penal*", Anales de Jurisprudencia, Año 8, Quinta época, Numero 234 Octubre - Diciembre. Uno de los métodos considerados para penalizar un acto consiste en exigir la intencionalidad de cometer el hecho delictivo, el querer y conocer el acto a ejecutar; como requisito adicional de la falta de autorización de la víctima.

Existe una relación causal, ya que éste último no podría sobrevenir si no fuese por el arranque inicial de intención, por la intención original de producir el hurto de identidad independientemente de que el resultado no fuese el esperado y sobrepase con mucho la magnitud del daño querido inicialmente.[36]

Sin Autorización O Ilegalmente.

Es menester que se excluyan los actos respaldados y legítimos a fin de garantizar que la tipificación del delito de Hurto de Identidad no afecte negativamente a la posibilidad de intercambiar información de identidad en la actividad empresarial cuando sea necesario. Sin embargo, como se ha indicado, descartar los actos en que la información utilizada ha sido revelada voluntariamente, podría excluir de la penalización actividades como la peska o el uso de información pública.

Se necesitan de estos elementos esenciales para establecer una disposición de derecho penal en que se defina una estructura.

3.2.3 PELIGROS PROVENIENTES DEL PROCESAMIENTO DE DATOS PERSONALES.

La tecnología puede introducir una serie de beneficios y de igual forma un inimaginable número de riesgos y peligros para las personas, los cuales suelen pasar desapercibidos e incluso volverse hasta llamativo por las facilidades que representa. No obstante esto, hay ocasiones en las cuales se suele canjear la libertad por la seguridad, por medio de la utilización de la tecnología, sin valorar las consecuencias que implica esta, a la cual, no se le niega que es una buena herramienta.

El moderno procesamiento de datos resulta ser no solo sutil y carente de violencia, sino, también, es seductor y apetecido. Sus peligros no suelen percibirse ya que los mismos se ocultan ante los beneficios que se obtienen. “Se vende el valiente nuevo mundo” con la promesa de mayor seguridad, menos burocracia, más eficacia y velocidad en las actividades de la agresiva sociedad de mercado. En este “mercadeo del futuro” se oculta el hecho del procesamiento de datos móvil y descentralizado, de la comercialización de la información, de la interconexión de los bancos de datos, y el papel del Estado de observador participante, el cual comprende mejor que antes, el hecho que ahora solo tiene que asegurarse un acceso a los bancos de datos particulares para

[36] Ibídem.

alcanzar la mayor parte de sus objetivos de control. El Ciudadano se encuentra aquí confuso y hasta desinformado, algo está pasando y él no lo comprende, ya que, lo que sucede se oculta en el vestido del avance y del progreso y contra esta promesa, una actitud reservada y meditativa tiene las peores cartas.[37]

Los datos personales que se comparten en las redes de la informática y por medio de la tecnología, implican peligros que se podrían entender como los daños colaterales en el derecho penal, ya que todo lo referente a la identidad de una persona, los gustos, costumbres, pasatiempos, sentimientos y emociones de una persona se vuelven públicas, por parte de ella misma.

Nos encontramos viviendo en la actualidad un alto índice de criminalidad, en la que el ciudadano vive atemorizado, esperando obtener protección por parte del Estado, sin ponerse a valorar que, en ese afán de ser protegidos, el Estado se vuelve invasivo de los datos personales de los ciudadanos, y que culmina con el desaliento de los ciudadanos al ver frustradas sus expectativas.

Las personas frente a estas funciones invasoras del Estado, tienen derecho a la protección frente al procesamiento de sus datos personales, lo cual, surge como una necesidad en el Estado de Derecho. De igual forma es importante reflexionar sobre los derechos y libertades públicas en juego, como también de las posibilidades de la persona humana en una sociedad tecnológica.

3.2.4 SURGIMIENTO DEL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA.

En las tecnologías de la informática y la comunicación, el concepto de intimidad se ve desvanecido, ya que, las personas en la necesidad de entablar relaciones personales, publican su información personal la que es susceptible de ser utilizada por criminales, generando retos para el derecho que tienen los ciudadanos de la protección de datos, y convirtiéndose en un iceberg para los controles sociales tradicionales, por lo que, en consecuencia es necesario crear mecanismos que le permitan al ciudadano garantizar su derecho de decidir, quién, cuando, donde, como y porque exhibe sus datos.

[37] Chirino Sánchez, Alfredo, Autodeterminación informativa y Estado de derecho en la sociedad tecnológica. CONAMAJ, San José, Costa Rica, 1997.

El autor Schamitt Glaeser, sostiene que una protección de la esfera de la vida privada es esencialmente una "protección de la información"[38], entendiéndose por esto que el ciudadano tiene la facultad de valorar que datos íntimos va a hacer públicos y cuales le puede afectar hacerlo.

Existen varios autores que han escrito al respecto sobre el derecho a la privacidad e intimidad que tienen los ciudadanos sobre sus informaciones, entre ellos Pérez Luño, que hace referencia a que la privacidad es una posibilidad del control de informaciones sobre sí mismo, de igual forma escribe el autor Lusky, sobre la invasión de la privacidad, concluyendo que este derecho no debe ser visto como un derecho de defensa, sino, como el derecho a evitar invasiones en su información personal que los medios tecnológicos implican.

Por último, es de tener claro que no nos estamos refiriendo a la limitación total de la utilización de los datos tecnológicos que la informática implica, sino, que debe existir una valoración del desarrollo futuro, lo cual lleva imbíbito el progreso de los Estados y que su utilización sea de una manera controlada por el ordenamiento jurídico vigente, determinando las consecuencias negativas de su uso inadecuado.

3.3 MÉTODOS QUE DERIVAN DE LA DIGITALIZACION PARA ADQUIRIR INFORMACIÓN.

La forma en que se obtiene la información, se convirtió en el cambio principal que introdujo el proceso de digitalización. Dándole a las redes sociales un plus de importancia que se utiliza para verificar e identificar procedimientos realizados en estas redes, teniendo en cuenta que la forma más común como es el robo de correspondencia, se convierte ahora hasta en complejas estafas, extorciones, delitos financieros, violación a la identidad y otros, sin olvidar la disponibilidad de la información referente a la identidad en las redes, en las cuales los usuarios hacen su publicaciones voluntariamente, donde dan a conocer ciertos datos que interesan a los delincuentes, los que utilizan dicha información robada para ejecutar actividades delictivas.

[38] Schamitt Glaeser, Walter, Schutz der privatssphare, en Isensee/kirchhof, Handbuch des staatsrechts, Heidelberg, Bd, VI, 1989. Pp 41 ss.

Dificulta describir el Hurto de Identidad *definiendo* los métodos utilizados para cometer el hecho delictivo, ya que por el avance tecnológico y el uso de redes sociales se ha facilitado el hurto de identidad, desde el clásico hurto de correspondencia hasta sofisticadas operaciones de peska.

Métodos tradicionales de defraudación.

Al largo de la historia figuran fraudes realizados con datos de identidad no digitales:

Reexpedición del correo: Que consiste en la remisión de correspondencia enviada a la víctima, facilitándole a los hechores obtener la información personal que se manda por correo siendo difícil que la víctima detecte actividades dudosas.

Hurto de correspondencia y de fuentes de información personal: Considerando que una gran cantidad de documentación de contenido importante, actualmente se siguen enviando por correo postal, este se convierte en un buen método, que permite la obtención de información relacionada a la identidad. Además de esta forma, existen otros blancos para el robo dirigido a obtener información relativa a la identidad, estas pueden ser: carteras, pasaportes, agendas, y otros artículos o documentos con información personal[39].

Ataques y amenazas internos: El éxito que han obtenido estos ataques obedece en gran parte al diseño de seguridad que se implementa, ya que son en un buen porcentaje para prevenir los ataques o amenazas que se puedan provocar desde el exterior, sin considerar que desde el interior se hace mas factible la obtención de información personal y que los empleados tienen la posibilidad de obtener incontables datos de instrumentos crediticios, así como tarjetas de crédito. -

Manejo de información pública: En las instituciones publicas y autónomas, existen registros públicos de contenidos completos con información personal, totalmente relacionada a la identidad y es por ello que para los delincuentes resulta fácil obtener estas fuentes de información con la finalidad de usos delictivos. -

[39] Marco, Gercke. Op cit, pág. 18

Defraudaciones Vinculadas A La Información Digital:

Así como ya se ha indicado, en el caso de la digitalización se considera que ha promovido la presencia de nuevos mecanismos para adquirir diversidad de información relacionada a la identidad. Vemos también la parte negativa de estos avances y como afecta a las instituciones responsables de hacer cumplir la ley, al mismo tiempo, la información digital que encontramos accesible a través de las tecnologías de la información, genera una variedad de ventajas a los delincuentes.

Mediante la tecnología informática y de las redes se le permite al delincuente la obtención de una gran cantidad de datos personales, sin realizar mucho esfuerzo. En la actualidad tenemos los siguientes tipos de defraudaciones:

a) Skimming: (copia de la tarjeta con un dispositivo de lectura de datos) En los últimos tiempos, la manipulación de cajeros automáticos para obtener información de la tarjeta de crédito de la víctima y sus códigos de acceso se ha convertido en un importante motivo de preocupación.[40]

b) Peska o pharming: El término "peska" se utiliza para describir los actos con los que se trata de inducir a la víctima mediante técnicas de ingeniería social a revelar datos personales o confidenciales. No es un delito nuevo, sino que desde hace decenios se lo conoce como "hurto mediante engaño". Si bien existen diferentes tipos de ataques de peska, los perpetrados a través del correo electrónico siguen tres etapas: en la primera, los delincuentes identifican a las compañías legítimas que ofrecen servicios en línea y que se comunican con sus clientes electrónicamente[41].

En la segunda, los delincuentes diseñan sitios web similares ("sitios falsos") a los sitios legítimos de la compañía considerada. Para dirigir a los usuarios a estos sitios falsos, los delincuentes con frecuencia envían correos electrónicos similares a los que envía la compañía legítima. Otra técnica utilizada para dirigir al usuario al sitio falso es la manipulación del sistema de nombres de dominio (DNS o SND), conocida como "pharming". En la tercera etapa, los delincuentes usan la información revelada por la

[40] Marco, Gercke. Op cit, pág. 19

[41] Marco, Gercke. Op cit., pag.19

víctima, por ejemplo, para entrar a sus cuentas y transferir dinero, solicitar pasaportes o abrir nuevas cuentas. El creciente número de ataques de este tipo llevados a cabo con éxito muestra la gravedad de la amenaza.

3.4 CONSECUENCIAS DE LA DIGITALIZACIÓN

La tecnología y sus avances en redes sociales han promovido el aumento del uso de información relacionada con la identidad, caracterizan la actual evolución del Derecho Penal [42] debido a las incomparables actividades que el ser humano realiza mediante sistemas automatizados de información, generalmente conectados a otros equipos o sistemas externos. El acceso a la información relacionada con la identidad de las victimas permite a los delincuentes intervenir en muchos ámbitos de su vida social, siendo ese motivo un blanco potencial para los delincuentes; es por ello que los riesgos del Derecho Penal del riesgo para la función de garantía del Derecho Penal son inmensos[43].

Las maneras más frecuentes de utilizar la información sobre la identidad figuran a continuación.

Comisión de delitos financieros.

La mayoría de veces el acceso a identificaciones relacionados con la victima permite al infractor cometer otros delitos, de ahí que los hechores no tengan como único interés la obtención de los datos, sino por la posibilidad de utilizarlos para actividades delictivas.

Por ejemplo, las personas que usan cuentas existentes de las víctimas, incluyendo cuentas de tarjetas de crédito, ahorro y de cheques, teléfono (teléfono fijo y servicio móvil), pago del servicio de Internet, correo electrónico y otras cuentas a las que estén suscritas en Internet, así como cuentas de seguros médicos; para hacer compras o realizar el pago de servicios, con cargo a las víctimas, así también pueden manejar cuentas financieras existentes o crear cuentas nuevas suplantando la identidad de la víctima, y realizar transferencias o compras con esas cuentas.

---

[42] Mendoza Buergo, Blanca. (2001). *El Derecho Penal en la sociedad del riesgo*. Editorial Civitas, Madrid. España. Pág. 21.

[43] Herzog, Félix. (1999). "*Algunos riesgos del Derecho Penal del riesgo*", en Revista Penal, Ed. Praxis en colaboración con la Universidad de Huelva, Salamanca y Castilla - La Mancha, Barcelona, Nro. 4. Pág. 54.

Venta de la información de la identidad

Otra modalidad es vender la información para su uso por otros infractores constituyéndose como motivación del delincuente el generar una ganancia directa sin cometer el delito para el cual se necesita la información obtenida, y venderlos posteriormente a otros infractores, que los utilizarán en nuevos delitos, Así, la información puede ser utilizada para abrir nuevas cuentas utilizando la información de las víctimas, por ejemplo cuentas para nuevos servicios de teléfono, tarjetas de crédito, solicitudes de préstamos o seguros de automóviles aprovechándose de las vulnerabilidades de las compañías de seguros, para conseguir créditos o adquirir bienes, que más tarde serán cobrados al verdadero titular de la información robada.

La usurpación de identidad.

Los perjuicios y menoscabos causados por el hurto de identidad no se limitan únicamente a problemas financieros, éste puede tener un alto costo tanto en el aspecto personal y sentimental de la víctima, debido a que puede dejar una sensación de violación a la vida privada; el apoderamiento consiste en no sólo hacerse de la cosa, sino en realizarlo sin derecho y sin consentimiento de la persona que pueda disponer de ella con arreglo a la ley.[44]

Las personas que hurtan la identidad pueden utilizar la información para ocultar su verdadera identidad, haciéndoles creer a terceros que es quien pretenden suplantar cuya finalidad es solicitar y usar instrumentos de identificación para inducir a error en las investigaciones, o usar la cuenta bancaria de la víctima para operaciones de blanqueo de dinero. Como un dato interesante es de recalcar que en el informe del Secretario General de las Naciones Unidas sobre las Recomendaciones para una estrategia mundial de lucha contra el terrorismo se destaca la importancia de diseñar mecanismos para reconocer el robo de identidad en la lucha contra el terrorismo o crimen organizado, porque los infractores pueden burlar las medidas de identificación y de prevención del terrorismo.

[44] González de la Vega, Francisco. (1988). *Derecho Penal mexicano, los delitos*. 22 edición. Editorial Porrúa. México. Pág. 251.

Así la delincuencia organizada en los últimos años ha tenido un crecimiento exponencial de sus actividades delictivas, afectando a toda la comunidad internacional y abarcando una gran cantidad de sectores de la actividad económica y social[45] desde luego, dañando sensiblemente la transferencia o el flujo internacional de datos mediante el apoderamiento ilegal de datos personales por grupos criminales perfectamente organizados y altamente especializados.

Falsificación de documento de identificación.

Además de la obtención o utilización indebida de información sobre la identidad, el acto de falsificar un documento que acredita la identidad de una persona puede considerarse un delito.[46]

Skimming.

Es la práctica que consiste en copiar datos personales contenidos en registros electrónicos como, por ejemplo, la banda magnética de las tarjetas de crédito, mediante pequeños dispositivos que leen la información allí registrada[47].

Uso no autorizado de datos de una tarjeta de crédito.

Consiste que de manera fraudulenta y sin buena fe, se posea, utilice, o permita a otra persona que utilice los datos de la tarjeta de crédito, incluida la información personal de autenticación, independientemente que los datos sean o no auténticos, obtener servicios proporcionados por el emisor de una tarjeta de crédito a los titulares de las tarjetas de crédito.

Como ejemplo y la forma más común de fraude de identidad es El "fraude de tarjetas de plástico" considerada como la principal forma de fraude de identidad en el Reino Unido por que la mayor parte de los gastos directos que se derivan de dicho fraude no los asume la víctima, sino las compañías emisoras de tarjetas de crédito, que posteriormente repercuten dichos costos en los titulares de la tarjeta, generalmente a

---

[45] Delgado Martín. J. (2001). *El proceso penal ante la criminalidad organizada.* Primera Edición. Editorial Bosch. Barcelona, España. Pág. 22.

[46] Marco, Gercke. Op cit. Pág. 81.

[47] Marco, Gercke. Op cit. Pág. 84.

través de altas tasas de interés. Algunas partes interesadas no consideran que se trate en realidad de un hurto de identidad, porque el acto en si no implica la suplantación de la personalidad de la víctima y en general las consecuencias para las víctimas son limitadas o fácilmente reparables. Sin embargo, el fraude de las tarjetas de pago provoca generalmente perjuicios considerables para las compañías defraudadas y los sistemas económicos, siendo hoy en días consideradas como victimas jurídicas.

Los titulares de cuentas individuales están menos protegidos del riesgo de resultar responsables de las pérdidas derivadas de este tipo de fraude, aunque el sector financiero va adoptando con frecuencia creciente códigos de buenas prácticas para poner a los consumidores a cubierto de responsabilidad por transacciones electrónicas fraudulentas.

3.5 DIVERSIDAD DE VÍCTIMAS DEL DELITO DE HURTO DE IDENTIDAD.

El robo de identidad es un delito que actualmente es mucho más fácil de cometer que antes, debido a las ventajas que el internet y la sistematización de datos personal ofrece para ello, sumado al descuido y la irresponsabilidad de los usuarios. Hoy en día las victimas de robo de identidad no son solo personas naturales, las empresas de igual forma se están viendo afectadas en gran medida por el robo de identidad de sus empleados.

La categorización lleva imbíbito la finalidad de elaborar posible reparación a las víctimas, ya que resulta difícil identificar que hayan sufrido los mismos daños por los diferentes tipos de perjuicios a cada uno, requiriendo medidas de reparación diferentes.

En el delito de hurto de identidad podemos encontrar una diversidad de víctimas (**particulares, empresas y gobiernos**).

3.5.1 LOS PARTICULARES.

Son las principales víctimas de los delitos relacionados con la identidad, debido a que su reputación es desvirtuada o utilizada indebidamente por el uso frecuente e irresponsable de las redes sociales.

El daño en los particulares se puede ver reflejado en:

Pérdidas financieras directas

Esta la pueden sufrir las víctimas individuales en forma de deudas originadas de modo fraudulento, honorarios conexos, gastos de mitigación del daño (por ejemplo, servicios de supervisión de créditos) y restablecimiento del historial, o pérdida del título de propiedad. El precio financiero derivado del delito relacionado con la identidad incluye graves perjuicios económicos, originada muchas veces por tasas de seguro y tasas de interés más altas, la denegación de crédito, la incapacidad de utilizar tarjetas de crédito existentes, la imposibilidad de obtener préstamos, la dificultad para obtener o acceder a cuentas bancarias.

Daños a la reputación.

Los efectos negativos en su reputación y las subsecuentes dificultades para restablecer su credibilidad, son cuestiones que lamentablemente afectan la vida del individuo a escala social, debido que cuando esta es hurtada y usurpada podría conllevar a un desgaste de su integridad, honestidad, porque podrían ser sujetos de infamia, calumnia, lo cual puede causar serias dificultades en su entorno social. El perjuicio causado puede tener consecuencias verdaderamente tremendas para las relaciones familiares o sociales, especialmente cuando las víctimas son detenidas por delitos que nunca cometieron.

Detención improcedente.

Numerosos ciudadanos han sido detenidos por delitos cometidos por otros, los cuales se hicieron pasar por ellos utilizando información de identidad robada.

Agencias de cobro que acosan a las victimas.

La forma de operar de estas agencias, es reclamar el pago de gastos reflejados en facturas, estados de cuenta o prestamos que las víctimas nunca realizaron y que desconocían, hasta el momento que procede el cobro.

3.5.2 LAS ENTIDADES PRIVADAS.

Las empresas son víctimas cuando sus identidades son objeto de apropiación indebida y se utilizan con fines no autorizados y fraudulentos. Dicho fraude de identidad empresarial se lleva a cabo para hacer caer en una trampa a alguien para que facilite sus

datos personales (por ejemplo, mediante la “peska”) o para obtener el producto de operaciones inmobiliarias o empresariales fraudulentas.

Un ejemplo en la perdida financiera empresarial es el uso de información de identidades fabricadas o identidades de personas fallecidas, para acceder a cuentas o abrirlas, con frecuencia las empresas indemnizan a los clientes afectados por las pérdidas correspondientes.

De todos los problemas de seguridad que puede experimentar una compañía, el robo de identidad es uno de los más preocupantes, ya que, puede dañar significativamente la reputación y las relaciones con clientes y proveedores, una modalidad muy usada últimamente para el robo de identidad a trabajadores de empresas y grandes compañías, se trata de suplantar a las marcas en redes sociales, engañan a los clientes, se lucran y dañan la reputación, lo mismo sucede con otras entidades no constituidas en Sociedad.

3.5.3 LOS GOBIERNOS.

También, los gobiernos son víctimas cuando los delincuentes utilizan sus servicios y prestaciones con fines fraudulentos. Los costos de ese fraude recaen a la larga en la población, precisamente en los contribuyentes.

3.5.4 VÍCTIMAS COLECTIVAS.

Estas se encuentran constituidas por la misma sociedad, como suele ocurrir en los delitos informáticos y otras defraudaciones, que suele denominarse delincuencia de cuello blanco. En todas estas infracciones destaca la despersonalización y colectivización, ya que crean en la colectividad inseguridad jurídica, temor o desconfianza en las tecnologías de la informática y comunicación.

Esto se debe a que en estos **delitos** se lesionan o ponen en peligro determinados bienes, cuya titularidad no corresponde únicamente a una **persona natural** o a una **persona jurídica**, sino que, además, a la comunidad o al Estado.

3.6 RESTABLECIMIENTO DE LA IDENTIDAD DE LA VÍCTIMA.

Quienes han sido víctimas del delito hurto de identidad, cuentan con una variedad de bases legales que pueden utilizar para que se les restituyan o puedan gozar de la reparación del perjuicio que se les ha causado. La legislación que regula la protección de los bienes jurídicos que perjudica este delito, puede ser nacional o internacional y entre ellas configuran los códigos, las leyes y las declaraciones de los "derechos de las víctimas"; la disponibilidad de medios de restitución por la vía penal; las causas suficientes de acción civil; y los derechos humanos relativos a la identidad, la privacidad y la reputación. A continuación, se examina cada una de esas bases.

Declaración de las Naciones Unidas sobre los principios fundamentales de justicia para las víctimas de delitos y del abuso de poder.

En 1985, la Asamblea General de las Naciones Unidas aprobó la Declaración sobre los principios fundamentales de justicia para las víctimas de delitos y del abuso de poder. Esta Declaración exhorta a los Estados Miembros a aplicar sus disposiciones, que se centran en la asistencia, el tratamiento y la reparación a las víctimas.

En la Declaración, el término "víctimas" se define con amplitud de modo que incluya las situaciones en las cuales no sea posible identificar, aprehender, juzgar o condenar al infractor, independientemente de la relación familiar que pueda existir entre él y la víctima. Sin embargo, al igual que otras declaraciones y textos legales sobre los derechos de las víctimas, se aplica únicamente a aquellas personas que hayan sufrido daños "como consecuencia de acciones u omisiones que violen la legislación penal vigente en los Estados Miembros". Así pues, en la medida en que los delitos relacionados con la identidad no se tipifiquen como tales en las legislaciones nacionales, la Declaración de las Naciones Unidas no resulta de gran utilidad.[48]

No obstante, la Declaración proporciona a las víctimas de delito en materia de identidad una base normativa sólida para solicitar asistencia del Estado y medidas

[48] Marco, Gercke. Op cit. Pág. 141.

facilitadoras del proceso de reparación, en particular cuando dichos delitos sean reconocidos como tales a nivel nacional.

Otras resoluciones, directrices internacionales, etc.

La resolución 2004/26 del Consejo Económico y Social de las Naciones Unidas sobre cooperación internacional en materia de prevención, investigación, enjuiciamiento y castigo del fraude, la falsificación de identidad y su uso indebido con fines delictivos y los delitos conexos alienta expresamente a los Estados Miembros a que "faciliten la identificación, la localización, el embargo preventivo, la incautación y el decomiso del producto del fraude y de la falsificación de identidad y su uso indebido con fines delictivos", entre otras medidas de carácter más preventivo. La restitución penal puede ser de utilidad para las víctimas en los casos en que los infractores sean procesados.

La Organización de Cooperación y Desarrollo Económicos (OCDE) ha publicado una serie de directrices y recomendaciones de interés dirigidas a sus Estados miembros, entre ellas las siguientes:

• Las Directrices de 1980 sobre la protección de la vida privada y la transmisión transfronteriza de datos personales (examinadas más detenidamente en el marco de la "Protección de datos").

• El Principio 2 de las Directrices de 2002 sobre la seguridad de los sistemas y redes de información, que hace hincapié en la responsabilidad de aquellos que diseñan, suministran y operan sistemas y redes de información, observando que "todos los participantes son responsables de la seguridad de los sistemas y redes de información" y que "los participantes deben ser responsables en cuanto corresponde a sus funciones individuales". Es decir, las víctimas individuales deberían tener que soportar pérdidas solamente en la medida en que sean responsables, y las entidades cuya conducta negligente contribuyó al hurto o fraude deberían asumir una parte equitativa de dichas pérdidas.

• Las Directrices de 2003 para la protección de los consumidores de prácticas comerciales transfronterizas fraudulentas y engañosas, las cuales establecen, entre otras cosas, que

los países miembros procurarán: "[establecer] mecanismos efectivos que permitan resarcir el daño causado a los consumidores víctimas de prácticas comerciales fraudulentas y engañosas"; y deberían "estudiar conjuntamente el efecto del resarcimiento al consumidor al enfrentar el problema de las prácticas comerciales fraudulentas y engañosas, prestando atención especial al desarrollo de sistemas efectivos de resarcimiento transfronterizo" [49].

3.7 LA RESPONSABILIDAD CIVIL DERIVADA DEL DELITO.

En lo que respecta a los llamados delitos informáticos existen dentro de estos los delitos cibereconómicos siento uno de ellos el delito de Hurto de Identidad en los que el ciberdelincuente lo que pretende es el apoderamiento del patrimonio, especialmente el dinero ajeno, mediante la utilización de técnicas informáticas, como delito de resultado que es, deriva consecuencias lesivas sobre el patrimonio de su víctima que originan responsabilidad civil.

Lo que no quiere decir que el delito de Hurto de Identidad implique únicamente apoderamiento patrimonial sino que además, la información, también es objeto del apoderamiento que se da en los delitos ciberintrusivos, aquellos en los que el ciberdelincuente lo que pretende es apoderarse de la información, datos y secretos que la víctima custodia en su ordenador, siendo susceptible una evaluación económica, que junto con el perjuicio causado por su conocimiento, deba igualmente generar responsabilidad civil.

La posibilidad de derivar de la acción penal ilícita la correspondiente responsabilidad civil conlleva igualmente a consideraciones procesales, ya que sólo los perjudicados u ofendidos por la infracción, podrán personarse como Acusación particular o Actor civil, debiendo el resto hacerlo en todo caso como Acción popular, desde luego no titular de derechos civiles de carácter resarcitorio, reparatorio ni indemnizatorio.

Se analiza aquí alguna peculiaridad a este respecto en lo que hace a los fraudes informáticos.

[49] Marco, Gercke. Op cit. Pág. 139.

Por lo demás, la causación de un delito o falta a través de vías telemáticas obliga a restituir la cosa, reparar los daños y a indemnizar los perjuicios causados por el hecho punible.

3.7.1 LA RESTITUCIÓN.

La responsabilidad civil reparatoria, se divide en dos fases: en primer lugar, se extiende a la restitución, obligando al hechor a devolver no sólo los efectos ocupados, sino a abonar también los menoscabos que se determinen judicialmente, dejando las cosas en el estado en que se encontraban antes de sufrir el ataque informático inicial. La restitución en los casos en que, no habido un menoscabo económico, obliga a la devolución de la información robada y a la destrucción de la transmitida indebidamente

3.7.2 RESARCIMIENTO DEL DAÑO.

El resarcimiento, como segunda manifestación de la responsabilidad, supone el conjunto de obligaciones de dar, hacer o no hacer, que se establecen judicialmente en función de la naturaleza del daño producido y de las condiciones personales y patrimoniales de su autor o responsable por culpa derivada consistiendo in eligendo, in vigilando o por enriquecimiento injusto.

Principalmente son los delitos que causan un daño patrimonial económico, los que dan lugar al resarcimiento y en especial los que generan desperfectos, como en el caso de los daños, en el que debe restaurar la situación precedente al ataque informático lesivo, reparando todos los desperfectos como cuando hubiere borrado, destruido, inutilizado o alterados softwares y en hardwares afectados, lo que incluye además de los ocasionados a la víctima buscada, los de todas las colaterales que no.

El juzgador deberá al menos intentar fijar los parámetros base para el cálculo de la restitución o retribución de estos complejos perjuicios en su esfera civil, pudiendo hacerlo estableciendo el posible resarcimiento a la víctima mediante el cálculo de:

- Realizar un cálculo del perjuicio de las cuotas que equivale en horas/dinero.

- Las pérdidas por el cese del funcionamiento del servicio.

- El daño emergente producido en la estima profesional o personal del ofendido.

- Fijar el costo de servicios alternativos usados o dejados de usar durante la acción criminal una vez pasado el intento de reacción.

- Determinar el costo de las demandas terceros que fueron afectados por los servicios no percibidos.

- Las indemnizaciones y exigencias ajenas directamente vinculadas a la acción delictiva.

- Establecer el lucro cesante en clientes nuevos perdidos a causa de la defraudación y otras derivaciones concausantes,

- El porcentaje de incremento económico adecuado dirigido a resarcir aquellos perjuicios que en esta materia son infinitamente difíciles, si no imposibles de demostrar, pero que obviamente concurren, ante la imposibilidad de singularizarlos.

3.7.3 RESARCIMIENTO DE PERJUICIOS MATERIALES Y MORALES.

El resarcimiento de perjuicios materiales y morales, puede ser fijado por el juez en sentencia, o en ejecución de ésta, además de los que se hayan causado al ofendido, los que se resulten a familiares y terceros. En este punto se incluye la obligación del sujeto de sufragar y acometer los costes de sacar de Internet las páginas delictivas de las que se haya servido para realizar su infracción, ya que al fin y al cabo es la técnica usada a través de Internet, la auténtica arma delictiva.

De igual manera es la vía de la reparación de perjuicios la que obliga en los delitos cibereconómicos a convertir en indemnización, o en trabajo equivalente, la evaluación no sólo del objetivo perjuicio sufrido por la víctima (daño emergente), sino también la del valor estimado (evaluable sobre prueba comprobable también) de los ingresos que el ataque informático ha impedido generar (lucro cesante) que en materia tan ligada a la producción intelectual, sobre todo de programas informáticos , conforma el verdadero caballo de batalla para la determinación de los montos indemnizatorios en este tipo de delitos, ya que en el delito de Hurto de Identidad se da la utilización de una identidad informática para poder obtener un lucro en perjuicio ajeno.

En los delitos vinculados a los ataques contra la propiedad intelectual o industrial a través de las nuevas tecnologías, en donde superada la barrera de las que lo son, y si nos encontramos ante lo que a veces se evidencian incontrolados ataques masivos cuasi-

industriales a la propiedad intelectual, lo más difícil es calcular las bases con las que dejar definitivamente zanjada la indemnización de los perjuicios ocasionados.

3.7.4 ESPECIFICIDADES DE LA RESPONSABILIDAD CIVIL EN MATERIA DE FRAUDES INFORMÁTICOS.

Dos son las víctimas de los Phishing y Pharming: por un lado, el propietario de los activos económicos defraudados es decir el titular de la cuenta bancaria atacada y de la que se detrae la sustracción, y por otro la entidad crediticia que opera a través de Internet el cual es el responsable de la seguridad sobre la misma.

El término “Phishing” (con la “Ph” en vez de la “F” propia del lenguaje de los crackers), se acuñó por primera vez en enero de 1996 en las noticias del grupo de hackers 2600. alt, y podría traducirse por “pesca de datos informáticos”. Es una acción delictiva compleja que en Internet se presenta mediante diferentes tipos de modalidades y que consiste en:

- El envío masivo de correos electrónicos, realizándose en ocasiones a través de enlaces a Páginas Web dirigidas a múltiples usuarios en los que suplantando e imitando la identidad, imagen o apariencia de una entidad o empresa financiera o bancaria y usando excusas relacionadas precisamente con la seguridad informática bancaria, solicita apremiante y urgentemente de quien los recibe que ceda sus datos bancarios personales de acceso a servicios de esta índole principalmente su clave de usuario, contraseña, número pin, aunque también la clave telefónica, el número de la tarjeta, fecha de caducidad, número de documentos personales, etc., de modo que como en la pesca quien “pica”, y los da, no hace sino ceder sus datos bancarios confidenciales a los estafadores (conocidos como “phishers” o ”scammers”) que de esta forma, y una vez conocidas las claves de su víctima (“phish”), realiza con ellas operaciones en la Red, normalmente transferencias bancarias o compras no consentidas e ignoradas a través de Internet, y a veces también retirada de efectivo en cajeros o duplicado de tarjetas con esos fines.

El "Pharming" aparece en abril de 2005 como consecuencia de fallos de seguridad que se detectaron por aquellas fechas en los servidores de Microsoft.

Consiste en manipulaciones técnicas de las direcciones DMS (Domain name server) que utiliza el usuario: de modo que (mecánicamente) le conducen a éste cuando las escribe en el navegador de Internet a páginas que no son la deseada, aunque aparentemente presentan un aspecto idéntico, y que han sido creadas por los delincuentes informáticos para conseguir la cesión no consentida de los datos confidenciales e información sensible y personal de la entidad de confianza de que se trate (bancaria, financiera, de venta de segunda mano, de subastas por Internet, de envío o intercambio de dinero al extranjero, etc.), y una vez en su poder, los atacantes quedan en condiciones de realizar los ilícitos e no consentidos apoderamientos patrimoniales sobre sus víctimas.

Consecuentemente, en primer lugar, por estar directamente afectadas, ambas pueden ser parte procesal acusadora en la causa penal por delito que se incoe.

Conseguiría parecer excesivo y inverso al sentido de las normas de las cláusulas generales de la contratación en esta modalidad bancaria que las entidades crediticias, en el curso de las reclamaciones oportunas, opusieran a su cliente su conducta negligente, porque sin la colaboración involuntaria del mismo, al menos en el Phishing que se diferencia del Pharming en que es una auténtica estafa sociológica, y el "scammer" no se habría apoderado de las claves de usuario y contraseña indispensables para la sustracción patrimonial posterior.

Sin embargo y normalmente hasta la fecha, el banco, o más propiamente sus aseguradoras, colaboran en la detección del ataque delictivo y han solido adelantar y reintegrar al cliente en el importe de la cantidad defraudada en estas modalidades de estafa informática en cuanto demuestran que han sido denunciadas, y todo a cambio de solicitar la colaboración procesal de la víctima cliente del banco.

En otras palabras, la existencia de esta delincuencia se vincula a problemas de seguridad propios a estos servicios bancarios, por lo general, como primera reacción quien asume inicialmente las consecuencias económicas del importe, inconsentida y fraudulentamente dispuesto, son las entidades bancarias.

Éstas, a su vez, en segundo lugar, tienen estos riesgos asegurados con sus entes aseguradores y/o con las Sociedades de Medios de Pago, quienes igualmente se las resarcen y devuelven, subrogándose en virtud del derecho el cual, el asegurador gana las

acciones y derechos del asegurado, ejerciendo una acción no autónoma que nace y existe en las mismas condiciones y circunstancias que tenía cuando el titular era el asegurado, de modo que recupera así su desembolso indemnizatorio, evita que se enriquezca injustamente el asegurado y sobre todo el causante del mal, devolviendo el sistema a su grado completo de justicia, actuando entonces en el proceso penal estos subrogados aseguradores como meros Actores Civiles.

En esta materia el Acuerdo no jurisdiccional internacional indica que cuando la entidad aseguradora tenga concertado un contrato de seguro con el perjudicado por el delito y satisfaga cantidades en virtud de tal contrato, sí puede reclamar frente al responsable penal en el seno del proceso penal que se siga contra el mismo, como actor civil, subrogándose en la posición del perjudicado.

Por otra parte, si la víctima hubiere contribuido con su conducta a la producción del daño o perjuicio sufrido los Jueces o Tribunales podrán moderar el importe de su reparación o indemnización, pues de tal tipo de concausas minorantes o reductoras de la reparación se deben excluir los artificios mendaces y las artimañas engañosas ínsitas en toda estafa, que sobrepasan con mucho el deber de diligencia que todo honrado ciudadano tiene contraído.

Lo contrario a lo que se inclinan a veces muchos moralizadores impropios de una jurisdicción como la penal supondría castigar la ingenuidad o la ambición de las víctimas de la estafa que no es lo querido por el legislador, pues se haya extramuros de los engaños no "bastantes" excluidos por el tipo y la descripción básica de la estafa.

De esta forma la cuestión de la intervención de las entidades bancarias y de sus aseguradoras, para subrogarse en el perjuicio de sus clientes se reduce a la demostración sociológica, tantas veces evidenciada en la obsolescencia de técnicas más securizadas de que los sistemas de telecomunicación informáticos no son perfectamente seguros, y claramente es así he ahí de la necesidad de regular tales conductas en nuestro país.

Así, aunque aparentemente, y uno a uno, los Phishing suponen ataques patrimoniales contra los usuarios de Internet, generan igualmente un ataque a la confianza depositada en esas empresas de diferente índole ya sean bancarias, de ventas, pagos, subastas, etc, por la Red y en el uso de Internet que, por ahora, ha desplazado el problema de la responsabilidad civil a las entidades, que reintegran lo estafado, pues más

o a la vez que un engaño al usuario, lo que hacen estos ataques es objetivar fallos y problemas en la seguridad informática que esas entidades deben corregir y evitar en primer término como son cambio del sistema de claves, uso de antimalware preventivo, campañas informativas, etc.[50]

3.8 MARCO JURÍDICO.

3.8.1 VISIONES INTERNACIONALES.

Hoy en día, ninguna de las organizaciones internacionales que se ocupan de temas relacionados con el derecho penal ha preparado instrumentos legislativos especiales sobre el Hurto de Identidad que contengan disposiciones para tipificar los actos pertinentes. Si bien, por un lado, no existen normas penales de alcance mundial[51], por otro, las organizaciones internacionales y regionales han intensificado sus actividades en este ámbito.

3.8.1.1 LAS NACIONES UNIDAS.

Los problemas planteados por los delitos relacionados con la identidad han cobrado una importancia primordial en el programa de prevención del delito y justicia penal de las Naciones Unidas. En la Declaración de Bangkok sobre "Sinergias y repuestas: alianzas estratégicas en materia de prevención del delito y justicia penal"[52], aprobada por la Asamblea General en su resolución 60/177, de 16 de diciembre de 2005, se destacó la importancia fundamental de combatir la falsificación de documentos y de identidad a fin de poner freno a la delincuencia organizada y el terrorismo. También se

[50] Los delitos informáticos: la reparación y las indemnizaciones. Especial referencia al fraude Por D. Eloy Velasco Núñez. http://www.elderecho.com/penal/informaticos-reparacion-indemnizaciones-Especial-referencia_11_194680019.htm (consultado en marzo de 2017).

[51]Carlos Alberto, Cerda A. (2016). Características del Derecho Internacional Penal y su clasificación entre Crimen y Simple Delito. Editora Working paper N° 64 Programa Derecho Internacional. Valparaíso, Chile. Pág. 5.

[52] La Declaración de Bangkok sobre "Sinergias y repuestas: alianzas estratégicas en materia de prevención del delito y justicia penal", 2005, aprobada por la Asamblea General en su resolución 60/177, de 16 de diciembre de 2005, se encuentra disponible en: http://www.un.org/events/11thcongress/declaration.htm (consultado en abril de 2017).

exhortó a los Estados Miembros a “mejorar la cooperación internacional, incluso a través de la asistencia técnica, para combatir la falsificación de documentos y de identidad, en particular la utilización fraudulenta de documentos de viaje, mejorando las medidas de seguridad”, así como a aprobar una legislación nacional apropiada. De conformidad con la resolución 2004/26 del Consejo Económico y Social (ECOSOC), la UNODC encargó la preparación de un estudio sobre “el fraude y la falsificación de identidad y su uso indebido con fines delictivos”, que fue publicado a principios de 2007.

El estudio siguió un enfoque más amplio que el adoptado por la OCDE. En primer lugar, la expresión general “delitos relacionados con la identidad” abarca toda clase de conductas ilícitas relacionadas con la identidad, incluidos los delitos de “falsificación de identidad” y “Hurto de Identidad”. En segundo lugar, se consideraron todos actos delictivos relacionados con el Hurto de Identidad, cometidos por medio de Internet o de otra forma, haciendo más hincapié en delitos y pautas más complejos debido a los vínculos existentes con la delincuencia organizada transnacional y otras actividades delictivas. Por último, los delitos relacionados con la identidad fueron considerados conjuntamente con el fraude, debido a su estrecha relación, así como a las instrucciones específicas al respecto del mandato del ECOSOC.

3.8.1.2 ORGANIZACIÓN DE COOPERACIÓN Y DESARROLLO ECONÓMICOS (OCDE).

En 1999, el Consejo de la OCDE aprobó un conjunto de directrices con miras a proteger el comercio electrónico que contenían medidas para la elaboración de estrategias de prevención del Hurto de Identidad[53]. Dado su carácter no vinculante, las directrices no contenían criterios que permitieran tipificar los aspectos específicos del Hurto de Identidad. En 2003, la OCDE elaboró otras directrices sobre aspectos del fraude transfronterizo. Al igual que las directrices de 1999, las de 2003 no abordaban específicamente un criterio para tipificar el Hurto de Identidad, pero se podían utilizar para

[53] Alma Rosa, Hernández M.; Karina, Rodríguez C. (2011). *La organización para la cooperación y el desarrollo económico, OCDE, y la definición de competencias en educación superior*. Editorial Educere, vol. 12, núm. 43, Pág. 75.

elaborar un marco más amplio que permitiera llevar a cabo investigaciones eficaces y procesar a los delincuentes.

3.8.1.3 LA UNIÓN EUROPEA.

La Unión Europea, ha elaborado diferentes instrumentos jurídicos que abordan la información relacionada con la identidad, como la Directiva de la Unión Europea sobre la privacidad, así como la tipificación de determinados aspectos del fraude y los delitos relacionados con Internet, como el acceso ilegal a los sistemas informáticos. No obstante, ninguno de ellos contiene disposiciones penales que aborden específicamente el Hurto de Identidad. Sin embargo, las dificultades que plantean las actividades delictivas conexas ya han sido reconocidas a nivel de la Unión Europea como una importante cuestión normativa.

Por su parte, la Comisión Europea indicó que "la cooperación policial y judicial en el seno de la Unión Europea se vería facilitada si el Hurto de Identidad se tipificara como delito en todos los Estados miembros". Esta propuesta allanó el camino para celebrar consultas con objeto de determinar si era necesario y conveniente que los Estados miembros promulgaran leyes específicas en la materia, ya que es razonable prever un creciente interés de la opinión pública europea por una prevención eficaz de los delitos relativos a la identidad. [54] En julio de 2007, la Comisión (DG Justicia, Libertad y Seguridad) inició un estudio comparativo sobre las definiciones de la expresión "Hurto de Identidad" utilizadas en los Estados miembros de la UE y sus consecuencias penales.

3.8.2 EL DELITO DE HURTO DE IDENTIDAD EN EL DERECHO COMPARADO.

En nuestra realidad el uso del Internet ha ocasionado el surgimiento de la identidad electrónica o identidad digital, que implica los datos personales sensibles que incluyen claves de acceso a cuentas bancarias o redes, por medio de los cuales las

[54] Antonio Pedro, Rodríguez B. (2011). *Los cibercrímenes en el espacio de libertad, seguridad y justicia.* Revista de Derecho Informático, núm. 103, Madrid, España. Pág. 12.

personas se comunican o utilizan en las redes informáticas y su circulación internacional es altamente peligrosa ante su posible apropiamiento no autorizado.

Es de tener presente que este tema no ha sido retomado de manera similar por los Estados internacionalmente hablando ya que han variado su regulación para ellos tenemos por ejemplo la definición aportada por Home Office Identity Fraud Steering Committe del Reino Unido, el hurto de identidad consiste en la recogida de información relativa a la identidad de una persona con el fin de obtener un fraude identitario, prescindiendo del hecho de que la víctima sea una persona viva o fallecida[55].

Es así que en diferentes países se ha tomado connotaciones propias relacionadas al delito de hurto de identidad informática, en el caso de México es regulado como el apropiamiento no autorizado de datos el cual adquiere un carácter penalista, cuando a través de redes digitales públicas o privadas de forma remota existe la posibilidad de que se adquieran mediante cracking referidos datos. En el lenguaje técnico penal, la palabra "apoderamiento" tiene un significado jurídico especial, particularmente en tipos penales, como el robo y el rapto[56]. En el robo, el apoderamiento consiste en no sólo hacerse de la cosa, sino en realizarlo sin derecho y sin consentimiento de la persona que pueda disponer de ella con arreglo a la ley, apropiamiento implicaría la aprehensión de las cosas en ausencia de todo consentimiento del sujeto pasivo.[57]

En los países europeos como son España, Francia y otros países tales como Italia, Alemania, Austria y Canadá el legislador decidió tipificar los delitos informáticos en su Código Penal, no existiendo una Ley Especial como ocurre en nuestro país, es así que en lo que respecta al derecho español específicamente lo regula el delito de Hurto de Identidad en el artículo 197 de su cuerpo penal arropan un sin número de supuestos al regular de manera general el derecho a la identidad, el derecho a la propia imagen, denotándose de la siguiente manera:

---

[55] http://www.identitytheft.org.uk/ (consultado en marzo 2017).

[56] Rodolfo, Romero Flores. Óp. Cit. Pág. 855.

[57] Francisco, González de la Vega (1988). *Derecho penal mexicano, los delitos*, 22ª. Ed., México, Porrúa. Pág. 251.

"Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero"

Con respecto a Colombia, al igual que en algunos países europeos no existe una ley especial que regule las conductas típicas penales, sino que se reformo el Código penal de dicho país, no existiendo una figura que regule específicamente el delito de Hurto de Identidad, sino únicamente a lo que se refiere a daños a sistemas informáticos, o ingreso inadecuado o desautorizado a los mismos, así como la divulgación de datos informáticos, pero cuando se presentan casos de suplantación de perfiles informáticos se acude a acciones constitucionales que protegen el derecho fundamental del buen nombre, por medio de la indemnización de daño moral.

En Argentina, se presentó un proyecto denominado 314 Ley sobre el Robo de Identidad Digital, en el cual se propone la incorporación del artículo 139 ter, al Código Penal argentino, el cual busca sancionar al que adoptare, creare, apropiare o utilizare, a través de Internet, cualquier sistema informático, o medio de comunicación, la identidad de una persona física o jurídica que no le pertenezca.

Con respecto a los Estados Unidos de América, en su legislación de orden federal se ha creado la Identity Theft and Asumption Deterrence Act,16 la cual trata sobre la disuasión de robo y asunción de identidad, promulgada por el Congreso en 1998, y fue codificada, en parte, en la sección & 1028 (a), título 18 del United States Criminal Code, la cual constituye la ley federal que hace del robo de identidad un delito. La norma penal decretada en este país se orienta a sancionar a quien transfiera, posea o utilice sin mediar autorización, los datos identificativos de una persona con el objeto de cometer, intentar o favorecer cualquier actividad ilícita. Así también, prácticamente la totalidad de los Estados de la Unión Americana han promulgado leyes relacionadas al delito de robo de identidad.

Se puede concluir que en lo relativo a la regulación jurídica y acciones en materia de robo de identidad promovidas por organismos internacionales, destaca a continuación lo emprendido por la Organización de las Naciones Unidas:

- Informe 2010 de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) denominado The Globalization Of Crime, A Transnational Organized Crime Threat Assessmen, en donde el capítulo 10 se relaciona con el cybercrimen, y, particularmente, el apartado 10.1 se vincula al robo de identidad.

- 12° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, realizado en Salvador, Brasil, durante abril de 2010, organizado por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), mismo que analizó la falta de cooperación internacional en materia de justicia penal, situación que propicia una vía de escape a los delincuentes cibernéticos, así como los vínculos entre la delincuencia organizada y la delincuencia cibernética.

- Informe 2007 de la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC), que contiene un apartado se dedica al análisis del robo de identidad.

- Consejo Económico y Social de la Organización de las Naciones Unidas, a través de la Comisión de Prevención del Delito y Justicia Penal, durante su 18° periodo de sesiones, celebrado en Viena del 16 al 24 de abril de 2009, se llevó a cabo un debate temático sobre el fraude económico y los delitos relacionados con la identidad.

- Consejo Económico y Social de la Organización de las Naciones Unidas, a través de su Comisión de Prevención del Delito y Justicia Penal, durante su 14° 315 periodo de sesiones, realizado en Viena del 23 al 27 de mayo de 2005, el tema 6 se orientó a la cooperación internacional en la lucha contra la delincuencia transnacional; el fraude y la falsificación de identidad y su uso indebido con fines delictivos. En la cual se presentaron los avances realizados por el grupo intergubernamental de expertos encargado de preparar un estudio sobre el fraude y la falsificación de identidad y su uso indebido con fines delictivos.

- Consejo Económico y Social de la Organización de las Naciones Unidas, mediante la Comisión de Prevención del Delito y Justicia Penal, durante su 13º periodo de sesiones, celebrado en 2004, examinó el problema desde una perspectiva de derecho penal y público, incluyendo el fraude comercial y otros tipos de fraude. También analizó el problema de la falsificación de identidad y su uso indebido con fines delictivos, que consistía en un problema conexo, y decidió solicitar que se efectuara un estudio combinado de ambos fenómenos, de modo que incluyera las relaciones entre el fraude y la falsificación de identidad y su uso indebido con fines delictivos y otros delitos, así como la prevención y control de referidos problemas recurriendo al derecho mercantil y al derecho penal.

- Consejo Económico y Social de la Organización de las Naciones Unidas, mediante la Resolución 2004/26 estableció directrices respecto de los elementos del estudio relacionados a la gama de delitos que suponen la falsificación de identidad.

- Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, misma que constituye la base jurídica aplicable en materia de cooperación en los casos de fraude transnacional vinculados en materia de robo de identidad[58].

3.9 MARCO NORMATIVO DE LA LEGISLACION SALVADOREÑA.

En este apartado trataremos de hacer un breve análisis sobre la regulación legal del delito de Hurto de Identidad en la Ley Especial de Delitos Informático y conexo, regulado en el Art. 22 del citado cuerpo legal el cual dispone:

"*Hurto de Identidad Art. 22.- El que suplantare o se apoderare de la identidad de una persona natural o jurídica por medio de las Tecnologías de la Información y la Comunicación, será sancionado con prisión de tres a cinco años. Si con la conducta descrita en el inciso anterior se daña, extorsiona, defrauda, injuria o amenaza a otra persona para ocasionar perjuicio u obtener beneficios para si mismo o para terceros y el apoderamiento recae sobre datos personales, confidenciales o sensibles definidos en la*

[58] Óp. Cit. Rodolfo, Romero F. Pág. 314 y 315.

Ley de Acceso a la Información Pública, será sancionado con prisión de cinco a ocho años".

Antonio E. Pérez Luño señala que quienes se han preocupado del tema, atendiendo a la novedad de la cuestión y el vertiginoso avance de la tecnología, han debido hacer referencia no sólo "a las conductas incriminadas de lege lata, sino a propuestas de lege ferenda, o sea, a programas de política criminal legislativa sobre aquellos comportamientos todavía impunes que se estima merecen la consiguiente tipificación penal". [59]

Ahora bien, cabe realizar un análisis desde la teoría del delito para determinar si cumple con los elementos típicos[60], para el caso iniciaremos con los elementos típicos del mismo, así para el caso podemos determinar que el delito informático de Hurto de Identidad deberá comprender los siguientes elementos:

3.9.1 ELEMENTO OBJETIVO

Consiste en la obtención, utilización o transferencia de datos de identificación personal de otra persona física o jurídica. Así mismo, la adopción, creación, apropiación o utilización de la identidad de tina persona física o jurídica que no le pertenezca.

3.9.2 ELEMENTO SUBJETIVO

Consiste en la voluntad de obtener, utilizar o transferir datos de identificación personal de otra persona; corno la de adoptar, crear, apropiarse o utilizar la identidad de otra persona a través de la internet o cualquier medio información cuya finalidad de causar un daño patrimonial y lo moral a la víctima.

3.9.3 BIEN JURÍDICO TUTELADO

En los delitos informáticos el bien jurídico protegido en general es la información, pero está considerada en diferentes formas, ya sea como un valor económico, como un valor intrínseco de la persona, por su fluidez y trafico jurídico, y, finalmente, por los

---

[59] Pérez Luño, Antonio E. (1996). "*Manual de informática y derecho*", Editorial Ariel S.A., Barcelona, España. Pág. 215.

[60] Tellez Valdés, Julio (2002). "*Los Delitos informáticos. Situación en México*", Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida. Pág. 24.

sistemas que la procesan o automatizan; los mismos que se equiparan a los bienes jurídicos protegidos tradicionales tales como:

EL PATRIMONIO, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar.

LA RESERVA, LA INTIMIDAD Y CONFIDENCIALIDAD DE LOS DATOS, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos.

LA SEGURIDAD O FIABILIDAD DEL TRAFICO JURÍDICO Y PROBATORIO, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos

EL DERECHO DE PROPIEDAD, en este caso sobre la información elementos físicos, materiales de un sistema informático, que es afectado por lo de daños y el llamado terrorismo informático.

Por tanto, el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde esta se almacena o transfiere.

3.9.4 SUJETOS QUE PARTICIPAN EN EL DELITO DE HURTO DE IDENTIDAD

Deben establecerse de forma específica los sujetos que participa, por lo que debe determinarse la responsabilidad penal de los autores y los cómplices. Vamos a establecer las características de los delincuentes informáticos (sujeto activo), como del sujeto sobre el que recae el ilícito penal (sujeto pasivo).

3.9.4.1 SUJETO ACTIVO

El sujeto activo la persona que realiza la prohibición establecida por la ley. Se debe tomar en cuenta como delincuentes informáticos no solo a sujetos con conocimientos especiales, que laboren o no dentro de la empresa afectada, sino a personas normales, sin mayores conocimientos en informática que pueden cometer conductas nocivas a sistemas informáticos desde sus hogares.

La red está siendo invadida por nuevos tipos de delincuentes, qué valiéndose de las características de esta, como el anonimato, por ejemplo, operan de un modo

desfavorable de la persecución de los individuos que realizan estas conductas. Así, una persona puede actuar con características distintas a las que originalmente posee, pudiendo alterar desde sus nombres hasta rasgos de su personalidad.

Los sujetos que cometen este tipo de ilícitos, son aquellas que poseen ciertas características, pero al mismo tiempo no presentan el denominador común de los delincuentes, pues los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos por su grado de participación en el delito pueden ser autores o cómplices como se encuentra regulado en el Código Penal.

Por lo que es cierto que muchos de los delitos se cometen desde dentro del sistema por personas que habitualmente lo operan y que tienen autorizado los accesos. Empero, las tendencias modernas apuntan hacia el campo de la teleinformática a través del mal uso del ciberespacio y las supercarreteras de la información o redes de telecomunicaciones; algunos estudiosos de la materia lo han catalogado como "delitos de cuello blanco", debido a que el sujeto activo que los comete es poseedor de cierto status socio económico; dentro de algunos sujetos activos en este tipo de delitos se encuentran:

Hackers, es la persona que se dedica a una tarea de investigación o desarrollo realizando esfuerzos más allá de los normales y convencionales, anteponiéndole un apasionamiento que supera su normal energía; el hacker es alguien que se apasiona por las computadoras, utilizando sus conocimientos en materia informáticas para poder ingresar sin autorización a los sistemas informáticos.

Crackers, es aquella persona que haciendo gala de grandes conocimientos sobre la computación y con un propósito de luchar contra lo que está prohibido, empieza a investigar la forma de bloquear las protecciones hasta lograr su objetivo. Este sujeto ingresa a los sistemas informáticos con la finalidad de causar dafio o apoderarse de los recursos del sistema o de la información contenida.

Phreacker, es una persona que con amplios conocimientos de telefonia puede llegar a realizar actividades no autorizadas con los teléfonos, por lo general con los celulares. Estos sujetos construyen equipos electrónicos que pueden interceptar y hasta ejecutar llamadas de aparatos telefónicos celulares sin que el titular se percate de ello.

3.9.4.2 SUJETO PASIVO

Es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto.

Debemos distinguir que sujeto pasivo o víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso del Hurto de Identidad las victimas pueden ser individuos, instituciones privadas, los gobiernos y sus instituciones públicas autónomas y descentralizadas, que utilizan sistemas automatizados de información, generalmente conectados a otros.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio del Hurto de Identidad, debido a que mediante el, podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casualmente por el desconocimiento del modus operandi de los sujetos activos.

3.9.5 COMPORTAMIENTOS NEUTROS COMO LIMITANTES JURIDICA DE LA APLICACION DEL TIPO PENAL DE HURTO DE IDENTIDAD.

La conducta punible es regulada por el Estado atendiendo a la necesidad de resguardar y de proteger bienes jurídico y se hace aplicando principios de lesividad y trascendencia de la conducta a efecto de mantener la convivencia social; por ello, se valora o analiza si el comportamiento debe de categorizarse como delito a través de la dogmática penal no obstante a ello el legislador se le puede presentar una diversidad de limitaciones de legislar o crear la norma ya sea por ausencia de regulación del comportamiento o carencia de una técnica legislativa apropiada.

En el caso del delito especial del Hurto de Identidad, aplicando tecnologías o medio informático se corre el riesgo que algunos comportamientos queden al margen de ese juicio de reproche, por lo que se vuelve imperativo diferenciar los niveles de responsabilidad en otras palabras autoría o participación del sujeto activo.

En este nivel de análisis sobre la forma de responsabilidad podemos advertir los comportamientos neutros, a tal efecto se entiende por estas las conductas que conllevan un aspecto de la intervención delictiva (pero no reconocida en la norma). Lo que en el Derecho Penal se conoce como *zona libre* de responsabilidad penal, ubicándose en el ámbito de lo comúnmente conocido como riesgo permitido. Con una terminología variada como, por ejemplo, «conductas neutrales»«conducta socialmente estereotipada»

«conductas cotidianas», «conductas inocuas» entre otras, se afirma que todo obrar neutral tiene la garantía *perse* de no ser punible, aun cuando, en algunos casos, puede en sí mismo coincidir fácticamente con una colaboración o favorecimiento a un delito cometido por otra persona.

La doctrina predominante en la actualidad fija a las conductas neutrales un tratamiento diverso, sin embargo, existe cierta coincidencia en el enfoque cuando dicha doctrina ubica el problema dentro de la categoría de la participación como elemento de responsabilidad, dándole una especie de grupo de casos que, en vista de su singularidad neutral, obliga un tratamiento diferenciado de los demás supuestos de inducción y complicidad como elemento de responsabilidad "participación", para disfrazar o evitar la impunidad de ese hecho.

Este procedimiento no es incorrecto, sin embargo, por esa vía las propuestas quedan expuestas a convertirse en meras soluciones ad-hoc, a modo de fichas sueltas de un pensamiento tópico, lejanas a una reflexión sistemática que ofrezca una solución en armonía con un sistema de la teoría del delito, por consiguiente, con un determinado sistema del Derecho Penal.

Relacionando la tesis anterior en la literatura penal, existe una diversidad de propuestas de solución a la problemática de las conductas neutrales. Haciendo un esfuerzo por sistematizarlas, resaltan dos grandes corrientes: una subjetiva y otra objetiva; de las cuales mencionamos los rasgos importantes.

Pero, antes de tratar ambas tendencias, conviene aclarar la diferenciación terminológica entre lo objetivo y lo subjetivo. Siguiendo en este punto lo alcanzado por el convencionalismo existente, se entiende de un modo general como «subjetivo» aquello que se relaciona con lo interno, con lo psíquico del hecho; mientras que lo «objetivo» se refiere concretamente a lo externo, que se sustrae a lo psíquico.

a) Teorías subjetivas

Lo interno está constituido por el dolo y la culpa, mientras que lo externo por la valoración social del hecho, o por la imputación objetiva. Para nuestro homenajeado, ambas perspectivas dan origen a la «posibilidad de distinguir la *imputación objetiva* de la *imputación subjetiva*. En la primera, lo relevante son las expectativas, vale decir, se pregunta si una persona de quien se esperaba determinada conducta la ha cumplido o no, sin interesar la identificación del sujeto que en el evento desarrolló la acción; lo que interesa es la conducta exigida a ese individuo, conducta que por supuesto es intencional como manifestación de querer. En cambio, en la imputación subjetiva sobresale el

aspecto individual del autor, no interesando por ejemplo la condición genérica de éste, sino si pudo prever o no el resultado, si realmente lo quizo o lo asintió como posible. más amplio, con la imputación objetiva se determina la vinculación entre un suceso y un querer, en tanto en la imputación subjetiva se investiga por el contenido de ese querer»

b) Teoría Objetiva.

A diferencia de las teorías subjetivas, las teorías objetivas colocan el juicio de valoración en el significado normativo del hecho, como algo que trasciende a la mente del autor, por manifestar en sí mismo una infracción normativa. Así, lo decisivo para la imputación jurídico-penal no es lo subjetivo, lo psíquico-real querido, sino el sentido objetivo de una conducta.

En el ámbito de las conductas neutrales, el pensamiento objetivista propone llevar a cabo el juicio de responsabilidad penal del acto de favorecimiento a un delito muy al margen de la disposición psíquica de los intervinientes, de manera que la punición o impunidad de la aportación mediante una actividad cotidiana dependa únicamente del sentido objetivo de infracción de la conducta.

3.9.6 DELITOS DE COMISION POR OMISION

Es de resaltar, que otra forma de comportamiento punible es la omisión, ósea, el deber de actuar cuando se ostenta la condición de garante, es esta condición la que implica responsabilidad por lo que se vuelve indispensable preguntarnos, ¿si en los delitos de Hurto de Identidad a través de los medios electrónicos, cabe la posibilidad de cometer esta acción mediante la modalidad omisiva?

Si atendemos en estricto sentido la definición conceptual de las acciones omisivas, diremos que: son aquellas que están vinculadas la producción de resultado por el elemento DE NO HABER EVITADO EL RESULTADO FINAL esto equivale según sentido de la ley, a su causación.

Por ello, es importante remitirnos al principio de legalidad en cuanto a establecer este supuesto como causa de responsabilidad; si no se ha reglamentado en la ley especial o en otra normativa, esta forma de actuar o acción, no es punitiva. Lo anterior lo podemos entender a través del siguiente ejemplo: *si el jefe de la unidad de registro y*

control de datos de los usuarios del sistema financiero tiene según la ley el deber de resguardar y cuidar celosamente los mismos y a través de una acción omisiva negligente, permite la extracción de los datos por otra persona este podría encontrarse en una posición de garante y consecuentemente derivaría en responsabilidad penal de acuerdo a su condición que posee. En el siguiente ejemplo, para reducir responsabilidad que la ley recoja o copile ese tipo de responsabilidad de no existir dicha norma, la misma carecería del juicio de reproche.

3.9.7 LOS EFECTOS JURÍDICOS DE LA TENTATIVA DEL DELITO DE HURTO DE IDENTIDAD A TRAVÉS DE MEDIOS INFORMÁTICOS Y TECNOLÓGICOS

Según nuestra normativa, delito tentado o imperfecto es aquel que no logra el resultado final por una acción extraña al agente que inicia el comportamiento, tendiente a obtener el resultado lesivo, aquí se nos presenta otro problema de dogmática en cuanto al delito de Hurto de Identidad a través de medios informáticos y tecnológicos, ya que, el artículo 22 de la Ley Especial, refiere en su inciso primero que la acción de sustraer o apoderarse de la información de una persona natural o jurídica, a través de las herramientas informáticas es responsable penalmente, aquí el legislador no exige un resultado material, si no, que reprime el hecho de apoderarse o sustraer la información, colocándonos en un delito de mera actividad y en este tipo de hechos la tentativa es suprimida, no se requiere como resultado para los actos de ejecución, un resultado lesivo por lo cual descalifica esta forma o modalidad de responsabilidad.

No así, acontece en la descripción de los elementos cualificantes del siguiente inciso, donde describe o relaciona la acción asociada a un resultado lesivo, sea este patrimonial o contra el honor; en este caso si los datos falsos no son ingresados a la red informática con el fin de obtener un provecho injusto no podría hacerse un reproche bajo esta modalidad, sino que implicaría la aplicación del inciso primero.

Estas son las dificultades de la aplicación práctica o de posibles errónea aplicación de este tipo penal por ser un tipo penal amplificado, pluriofensivo y complejo; en tal sentido, podríamos aseverar como grupo que la aplicación de la tentativa es inaplicable en este delito**.**

3.9.8 LA PARTE GENERAL Y SU APLICACIÓN EN LA LEY ESPECIAL SOBRE LOS DELITOS INFORMATICOS Y CONEXOS.

Las disposiciones generales del código penal son aplicable a la presente normativa su condición de especialidad y especificidad cuando dichas regulaciones no riñan con la ley especial, por lo tanto, podemos aseverar que la autorización de ley para su debida aplicación lo contempla el articulo 6 cuando sostiene que los principios fundamentales del Código Penal serán aplicables siempre que las normas generales a los hechos punibles previstos en leyes especiales no contravengan su espíritu y riñan con las mismas, dado que todo hecho punible descansa su reglamentación en los siguientes principios: **a)** legalidad, **b)** dignidad humana, **c)** lesividad, **d)** responsabilidad, **e)** necesidad, etc.

Asimismo, las diferentes formas de responsabilidad que regula el título II capítulo I de dicho cuerpo legal, en tal sentido, podemos afirmar que la observancia de esta disposición de la ley penal se vuelve de obligatorio cumplimiento y de existir conflicto entre una y la otra, la solución en la aplicación de un caso en concreto, deberá hacerse en amparo a la ley especial. Los posibles problemas que podrían generarse en la aplicación de un caso práctico, seria, las formas de responsabilidad, pero en este caso la ley especial deberá reglamentar o codificar las mismas.

3.9.9 OBLIGACIONES JURIDICAS INTERNAS DEL ESTADO EN LA PROTECCION DE LOS DELITOS INFORMATICOS.

El estado como garante de la protección y tutela jurídica, colectivos o individuales debe de codificar o reglamentar aquellas conductas que transgredan el orden social, ya que, para mantener el equilibrio jurídico entre Estado y ciudadano debe forzar jurídicamente al individuo a observar y respetar las normas de convivencia, por ello, dado el avance de las nuevas tecnologías y su uso en delitos utilizando el espacio digital se vuelve indispensable y obligatorio regular y reglamentar las posibles conductas punibles en el uso de estas tecnologías informáticas.

Situación que conlleva la obligación del Estado de realizar las siguientes acciones:

- **a)** Identificación de los comportamientos lesivos no regulados.
- **b)** Formulación a través de una técnica legislativa apropiada que codifique los delitos informáticos (políticas de represión)

c) Resarcimientos patrimonial y moral de las víctimas de los delitos informáticos.

d) Creación de organismos especializados en la investigación y persecución de esta clase de delitos.

El Estado de El Salvador como miembro parte de la organización de las Naciones Unidas ha asumido frente a la Comunidad Internacional la obligación de ajustar su ordenamiento jurídico interno a los instrumentos internacionales, específicamente (EL CONVENIO SOBRE LA CIBERDELINCUENCIA, CONVENIO DE BUDAPEST), en donde se le conmina a crear una ley especial que copile aquellas conductas susceptibles de ser calificadas como ciberdelincuencia.

3.9.10 DESVENTAJAS Y VENTAJAS DE LA CODIFICACION

3.9.10.1 DESVENTAJAS DE LA CODIFICACION

Dentro de las desventajas de la codificación de conductas especiales como lo son delitos informáticos o ciberdelitos podemos señalar las posibles que podrían ser.

a) Conflictos aparentes de normas, ósea que una conducta especial podría adecuarse dentro el ordenamiento interno por dos o más tipos penales.

En el caso de El Salvador, existen delitos codificados en la norma penal que podrían ser susceptibles a la vez de ser calificado en la ley especial, esto podría presentar una limitación en la aplicación práctica de los ciberdelitos.

b) La supresión u omisión de las diferentes formas de responsabilidad penal al generar una confusión al momento de juzgar y sancionar por parte del juzgador este tipo de delito, por ejemplo: en los casos de las conductas neutras, la comisión por omisión y atendiendo el resultado final (la tentativa).

3.9.10.2 VENTAJAS DE LA CODIFICACION.

Las ventajas de la codificación de estas conductas en una ley especial es el tratamiento integral y específico a esas formas de delincuencia informática, ya que, al existir un sistema de normas dispersas podría cometerse el error de un tratamiento punitivo inapropiado el cual se resuelve al existir una normativa especial, dándole preeminencia en su aplicación.

3.9.11 PROBLEMAS CONCURSALES EN TORNO A LOS DELITOS DE RESULTADO Y LOS PREVISTOS EN EL INCISO SEGUNDO DEL ARTICULO 22 DE LA LEY ESPECIAL DE DELITOS INFORMATICOS Y CONEXOS.

En torno a posibles problemas concursales en la aplicación de la norma debemos acotar que los mismos no existen, dado que la disposición del art 22 de la Ley Especial es claro en definir la forma de materializar la acción punitiva, el tipo penal en su inciso primero refiere el apoderamiento, y suplantación de la identidad ajena mediante medios tecnológicos; esta simple acción conlleva una responsabilidad penal sin asociarla y vincularla a un resultado material. El legislador sanciona exclusivamente la acción de apoderamiento o suplantación sin un fin, dosificando el reproche del injusto.

Ahora bien, el inciso segundo de la normativa asocia la acción del inciso primero a un fin o a un resultado, ósea, no sola la simple acción de suplantar o apoderase, sino también, que la misma sirva para cometer un resultado lesivo, por ello podemos afirmar que la norma es complementaria a una acción de mera actividad como lo es el simple hecho de tener o poseer una identidad ajena. Ya que al fijar la dosificación de la pena por el uso de esta identidad ajena el legislador pondera el resultado material, es decir, el daño al patrimonio o al honor.

Por lo cual, aseveramos que no existe un problema concursal en la disposición aludida, sino, lo que se hace es complementar la acción a la dosificación justa y razonable del efecto material del delito.

Por ello, podemos afirmar que efectivamente queda absorbida la conducta del primer inciso con las del inciso segundo de la referida ley.

3.9.12 ELEMENTOS AMPLIFICADORES DEL TIPO PENAL DE HURTO DE IDENTIDAD EN LA NORMATIVA ESPECIAL DE DELITOS INFORMATICOS.

Con anterioridad se ha señalado que la disposición que describe el tipo penal básico también establece elementos amplificadores de la responsabilidad, así, la justo proporción al reproche penal de los diversos comportamientos regulados en esta. Ya que establece dos respuestas penales distintas, la regula el inciso primero y las amplificadas en el inciso segundo; al observar la respuesta penal o dosificación de la conducta se puede concluir que el inciso segundo cualifica y dosifica la respuesta incrementándose esta por razón del resultado lesivo.

En este tópico también se vuelve indispensable resolver la pregunta referida a los problemas prácticos que provocan las conductas neutras en el tipo penal, como lo advertimos en un ítem anterior, referimos que las conductas neutras conllevan un aspecto de la intervención delictiva (pero no reconocida en la norma). Lo que en el Derecho penal se conoce como *zona libre* de responsabilidad penal, ubicándose en el ámbito de lo comúnmente conocido como riesgo permitido.

En este caso podemos afirmar que, a la luz del principio de legalidad a las conductas neutras, no se les reconoce sentido punible, es decir, que no serán merecedoras de un reproche por carecer de una regulación formal y material.

3.10 DEFINICIÓN Y OPERACIONALIZACIÓN DE TÉRMINOS BÁSICOS.

a) Delito Informático: se considerará la comisión de este delito, cuando se haga uso de las tecnologías de la información y la comunicación, (TIC) teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información.

b) Bien Jurídico Protegido: es la información que garantice y proteja el ejercicio de derechos fundamentales como la intimidad, honor, integridad sexual, propiedad, propiedad intelectual, seguridad pública, entre otros.

c) Datos Informáticos: es cualquier representación de hechos, información o conceptos en un formato digital o análogos, que puedan ser almacenados, procesados o transmitidos en un sistema informático, cualquiera que sea su ubicación, así como las características y especificaciones que permiten describir, identificar, descubrir, valorar y administrar los datos;

d) Medio de Almacenamiento de Datos Informáticos: es cualquier dispositivo a partir del cual la información es capaz de ser leída, grabada, reproducida o transmitida con o sin la ayuda de cualquier otro medio idóneo;

e) Sistema Informático: es un elemento o grupo de elementos interconectados o relacionados, pudiendo ser electrónicos, programas informáticos, enlaces de comunicación o la tecnología que en el futuro los reemplace, orientados al tratamiento y administración de datos e información.

f) Comunicación Electrónica: es toda transmisión de datos informáticos, cuyo contenido puede consistir en audio, texto, imágenes, videos, caracteres alfanuméricos, signos, gráficos de diversa índole o cualquier otra forma de expresión equivalente, entre un remitente y un destinatario a través de un sistema informático y las demás relacionadas con las tecnologías de la información y la comunicación.

g) Dispositivo: es cualquier mecanismo, instrumento, aparato, medio que se utiliza o puede ser utilizado para ejecutar cualquier función de la tecnología de la información y la comunicación.

h) Interceptar: es la acción de apropiarse, interrumpir, escuchar o grabar datos informáticos contenidos o transmitidos en cualquier medio informático antes de llegar a su destino.

i) Programa Informático: es la rutina o secuencia de instrucciones en un lenguaje informático determinado que se ejecuta en un sistema informático, pudiendo ser éste un ordenador, servidor o cualquier dispositivo, con el propósito que realice el procesamiento y comunicación de los datos informáticos.

j) Proveedor de Servicios: es la persona natural o jurídica que ofrece uno o mas servicios de información o comunicación por medio de sistemas informáticos, procesamiento o almacenamiento de datos.

k) Tráfico de Datos Informáticos: son aquellos que se transmiten por cualquier medio tecnológico, pudiendo mostrar el origen, destino, ruta, hora, fecha, tamaño, duración de la comunicación, entre otros.

l) Tecnologías de la información y la comunicación: es el conjunto de tecnologías que permiten el tratamiento, la comunicación de los datos, el registro, presentación, creación, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información en forma automática, de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética, entre otros.

m) Datos Personales: es la información privada concerniente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico u otra similar.

n) Datos Personales Sensibles: son los que corresponden a una persona en lo referente al credo, religión, origen étnico, filiación o ideologías políticas, afiliación sindical, preferencias sexuales, salud física y mental, situación moral, familiar y otras informaciones íntimas de similar naturaleza o que pudieran afectar el derecho al honor, a la propia imagen, a la intimidad personal y familiar.

o) Redes Sociales: es la estructura o comunidad virtual que hace uso de medios tecnológicos y de la comunicación para acceder, establecer y mantener algún tipo de vínculo o relación, mediante el intercambio de información.

3.11 SISTEMA DE HIPÓTESIS.

3.11.1 HIPÓTESIS GENERAL.

- Para lograr la persecución y sanción de las incidencias del delito de Hurto de Identidad de la Ley de delitos informáticos, será necesaria la aplicación de técnicas investigativas de tecnología avanzada.

3.11.2 HIPÓTESIS ESPECÍFICAS.

- La escueta descripción de los elementos normativos del delito de Hurto de Identidad conlleva a la errónea interpretación del tipo penal en las diversas modalidades delictivas por parte de los aplicadores de justicia en el proceso penal salvadoreño.

- El delito de Hurto de Identidad protege multiplicidad de bienes jurídicos, entre estos el honor, la imagen, la intimidad, por lo que su íntima interconexión con otros delitos conexos que protegen esos mismos bienes jurídicos, genera problemas interpretativos para la adecuación de las múltiples conductas al tipo penal de Hurto de Identidad en el sistema jurídico salvadoreño.

- La aplicación de la teoría de la disponibilidad para la configuración del delito de Hurto de Identidad es un elemento esencial para dar por consumado el delito por parte del sujeto activo del mismo, lo que representaría problemas para la acreditación en el sistema investigativo del delito, adecuándolo a nuevas modalidades modernas de ejecución del tipo penal.

CAPITULO IV

4. HALLAZGO EN LA INVESTIGACION.

4.1 PRESENTACIÓN Y DISCUSIÓN DE RESULTADOS.

En el presente capítulo se presentarán los datos y resultados obtenidos por medio de la implementación de técnicas e instrumentos de investigación, realizando una descripción individualizada de cada uno de ellos, así como el análisis de los resultados obtenidos., dando con ello cumplimiento a los Objetivos Específicos planteados en la investigación.

En relación al primer Objetivo Especifico, se cumple por medio de la realización de una encuesta la cual fue proporcionada y resuelta por distintas entidades del sistema de justicia de El Salvador, específicamente en la Zona Oriental (Jueces, Auxiliares Fiscales, Defensores Particulares como Defensores Públicos, Agentes de la policía Nacional Civil), obteniendo con ello un esquema o percepción de la problemática investigada.

OBJETIVO ESPECIFICO I: Determinar las prácticas de las conductas delictivas realizadas por medio del delito de Hurto de Identidad.

PREGUNTAS DE LAS ENCUESTAS REALIZADAS.

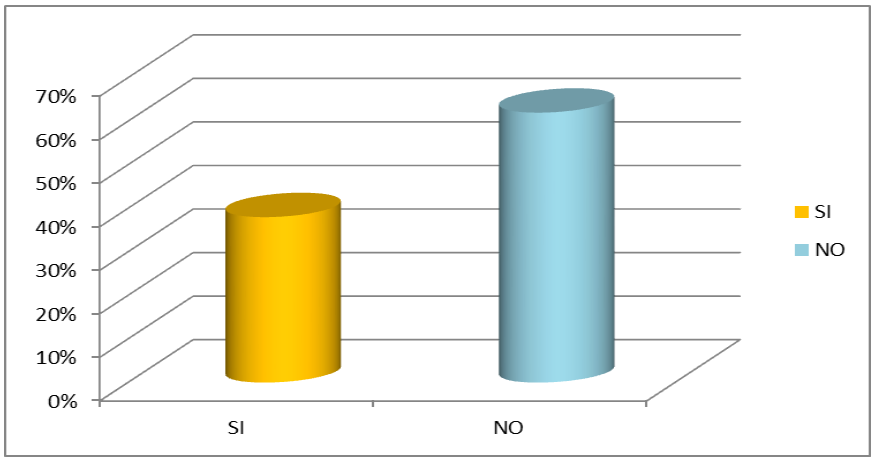
¿Conoce cuáles son los elementos típicos del delito de hurto de identidad que se deben reunir para configurarlo como tal?

Tabla I: Elementos típicos del delito de hurto de identidad

ALTERNATIVA DE RESPUESTA	RESPUESTA	FRECUENCIA
SI	19	38%
NO	31	62%
TOTAL	50	100%

Fuente: Tabla elaborada por equipo investigador

Grafico I: Elementos típicos del delito de hurto de identidad



Fuente: Gráfico elaborada por equipo investigador

Interpretación de resultados: El 38% de las personas encuestadas respondieron que si conocen cuales son los elementos típicos del delito de hurto de identidad ("el que suplantare o se apoderare" de la identidad de una persona natural o jurídica), para que este se configure como tal, mientras que el 62% respondió que no, lo que nos indica que es un alto porcentaje de los ciudadanos que desconoce cuándo están realizando o están siendo perjudicados en su intimidad, así como víctimas o responsables de cometer el delito cibernético de hurto de identidad. -

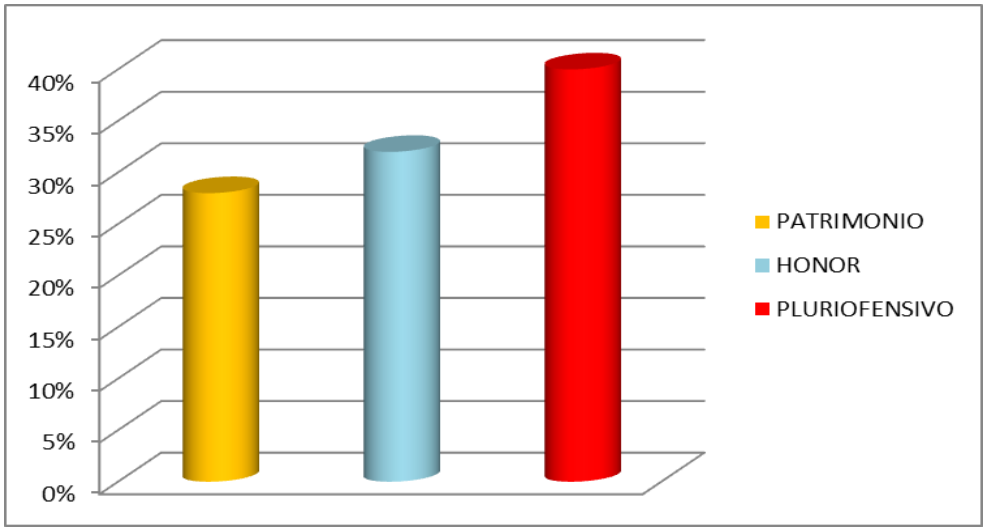
¿Cuál o cuáles son los bienes jurídicos que protege el delito de hurto de identidad en la Ley Especial de Delitos Informático y conexos?

Tabla II: Bienes jurídicos que protege el delito de hurto de identidad en la Ley Especial de Delitos Informático y conexos

ALTERNATIVA DE RESPUESTA	RESPUESTA	FRECUENCIA
PATRIMONIO	14	28%
HONOR	16	32%
PLURIOFENSIVO	20	40%
TOTAL	50	100%

Fuente: Tabla elaborada por equipo investigador

Grafico II: Bienes jurídicos que protege el delito de hurto de identidad en la Ley Especial de Delitos Informático y conexos. -



Fuente: Gráfico elaborado por equipo investigador

Interpretación de resultados: En la muestra de la encuesta sobre los bienes jurídicos protegidos por la Ley Especial de Delitos Informáticos y conexos, se identifico que, el 28% conoce que uno de los bienes jurídicos protegidos es el bien jurídico del patrimonio, el 32% conoce sobre el honor, mientras que el 40% considera que este delito puede perjudicar varios bienes jurídicos, considerándolo como pluriofensivo, el cual es muy acertado, ya que por la característica de la conducta realizada por cometimiento de este ilícito se pueden consumar otros delitos comunes descritos en el Código Penal, como la daños, extorción, defraudación, injuria y amenaza.

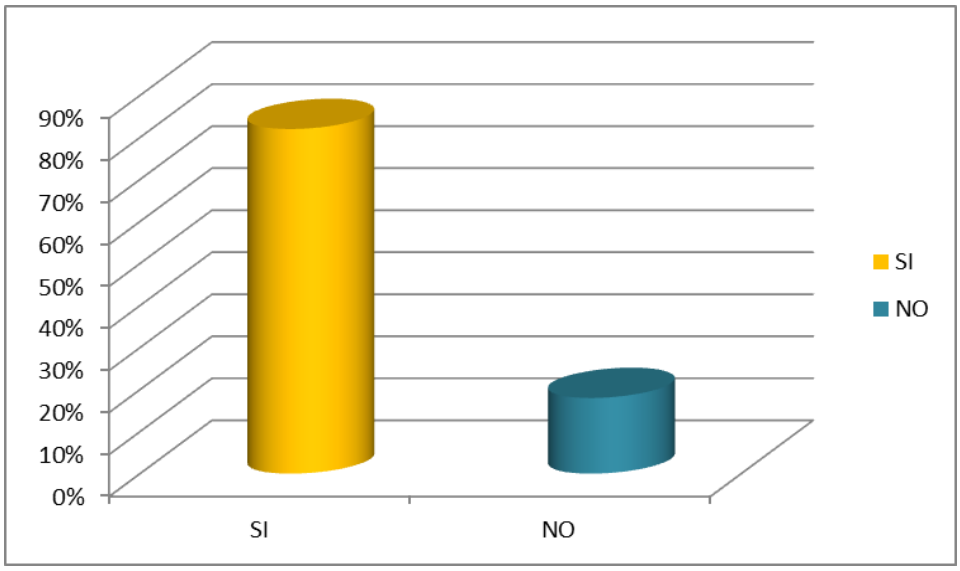
¿Para usted admite tentativa el delito de hurto de identidad?

Tabla III: Admisión de tentativa el delito de hurto de identidad. -

ALTERNATIVA DE RESPUESTA	RESPUESTA	FRECUENCIA
SI	41	82%
NO	9	18%
TOTAL	50	100%

Fuente: Tabla elaborada por equipo investigador

Grafico III: Admisión de tentativa el delito de hurto de identidad



Fuente: Gráfico elaborado por equipo investigador

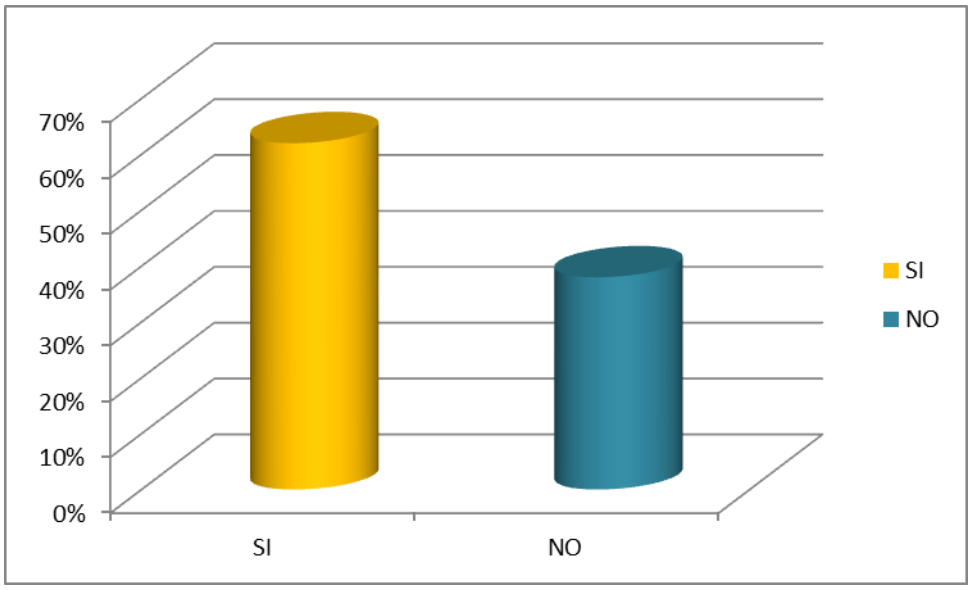
Interpretación de resultados: En relación a la tentativa del delito de hurto de identidad, el 82% de los encuestados considera que este delito admite tentativa, mientras que el 18% dijo que no, por lo tanto debemos interpretar que existe un conocimiento acertado que en este ilícito, si se puede dar la tentativa, al haber constituido los actos ejecutivos, es decir, que se pudieron haber realizado algunos o todos, pero siempre encaminados a la realización de hurto de identidad y si este no se llegara a consumar por causas ajenas al sujeto activo.

¿Existen a su criterio problemas en las técnicas de investigación que implicaría acreditar autoría y participación del sujeto activo del delito de hurto de identidad?

Tabla IV: Problemas en las técnicas de investigación que implicaría acreditar autoría y participación del sujeto activo del delito de hurto de identidad

ALTERNATIVA DE RESPUESTA	RESPUESTA	FRECUENCIA
SI	34	62%
NO	16	38%
TOTAL	50	100%

Fuente: Tabla elaborada por equipo investigador



Fuente: Gráfico elaborado por equipo investigador

Grafico IV: Problemas en las técnicas de investigación que implicaría acreditar autoría y participación del sujeto activo del delito de hurto de identidad.-

Interpretación de resultados: 62% de la población encuestada considera, que si existen problemas en las técnicas de investigación que implica acreditar autoría y participación del sujeto activo del delito de hurto de identidad, mientras que el 38% respondió que no, por lo que se detecta que el problema de persecución y enjuiciamiento de este delito según los resultados de la encuesta radican en gran parte por la falta de precisión y aplicación de las técnicas de investigación.-

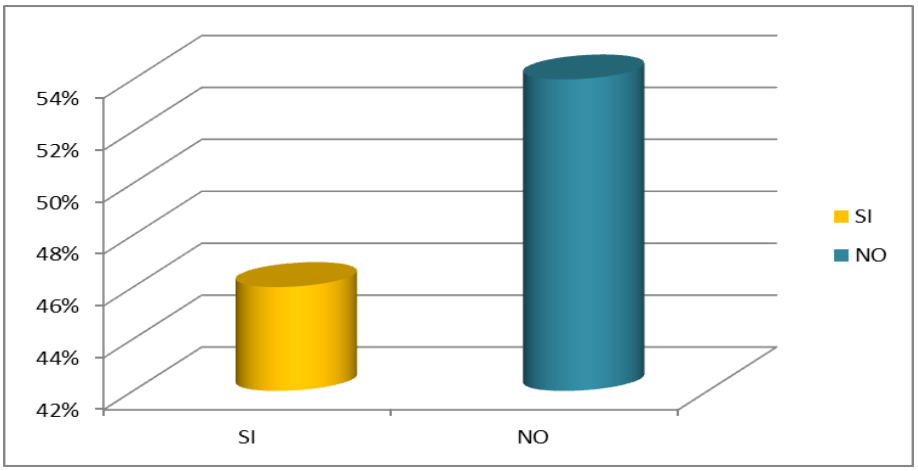
¿Es preciso el artículo 22 de la Ley Especial de Delitos Informático y Conexos, en delimitar la descripción típica del delito de hurto de identidad?

Tabla V: Descripción típica del delito de hurto de identidad en artículo 22 de la Ley Especial de Delitos Informático y Conexos

ALTERNATIVA DE RESPUESTA	RESPUESTA	FRECUENCIA
SI	23	46%
NO	27	54%
TOTAL	50	100%

Fuente: Tabla elaborada por equipo investigador

Grafico V: Descripción típica del delito de hurto de identidad en artículo 22 de la Ley Especial de Delitos Informático y Conexos.-



Fuente: Gráfico elaborado por equipo investigador

Interpretación de resultados: el 46% respondio que el artículo 22 de la Ley Especial de Delitos Informático y Conexos, es preciso en delimitar la descripción típica del delito de hurto de identidad, mientras que el 54% dijo que no. Lo que significa que para la mayoría de encuestados no tiene claridad sobre el elemento típico de dicho delito, lo que puede generar confusión al momento de determinar y probar su existencia.-

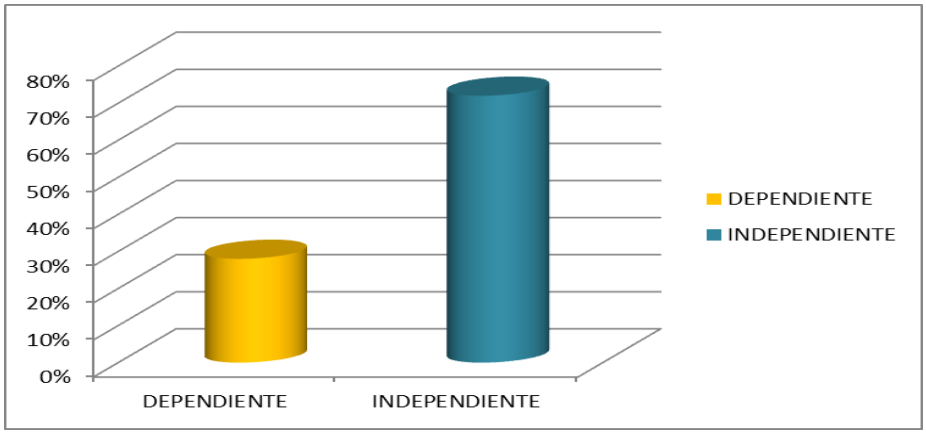
¿Es un delito independiente o dependiente el delito de hurto de identidad regulado en el Art. 22 de la Ley Especial de Delitos Informático y conexos, con el delito hurto básico que regula el art. 207 del Código Penal?

Tabla VI: Dependencia entre el delito de Hurto de Identidad contemplado en el art. 22 de la Ley Especial de Delitos Informáticos y conexos, con el delito de Hurto básico, regulado en el art. 207 del Código Penal.

ALTERNATIVA DE RESPUESTA	RESPUESTA	FRECUENCIA
DEPENDIENTE	14	28%
INDEPENDIENTE	36	72%
TOTAL	50	100%

Fuente: Tabla elaborada por equipo investigador

Grafico VI: Dependencia entre el delito de Hurto de Identidad contemplado en el art. 22 de la Ley Especial de Delitos Informáticos y conexos, con el delito de Hurto básico, regulado en el art. 207 del Código Penal.



Fuente: Gráfico elaborado por equipo investigador

Interpretación de resultados: El 28% de las respuestas obtenidas en la encuesta consideran que el delito hurto de identidad, regulado en el Art. 22 de la Ley Especial de Delitos Informático y conexos, es dependiente con el delito hurto básico que regula el art. 207 del Código Penal, mientras que el 72% lo valora como un delito independiente, ya que la ejecución del primero no depende en ningún sentido del supuesto de hecho, ni de la consecuencia jurídica del hurto regulado en el Código Penal.

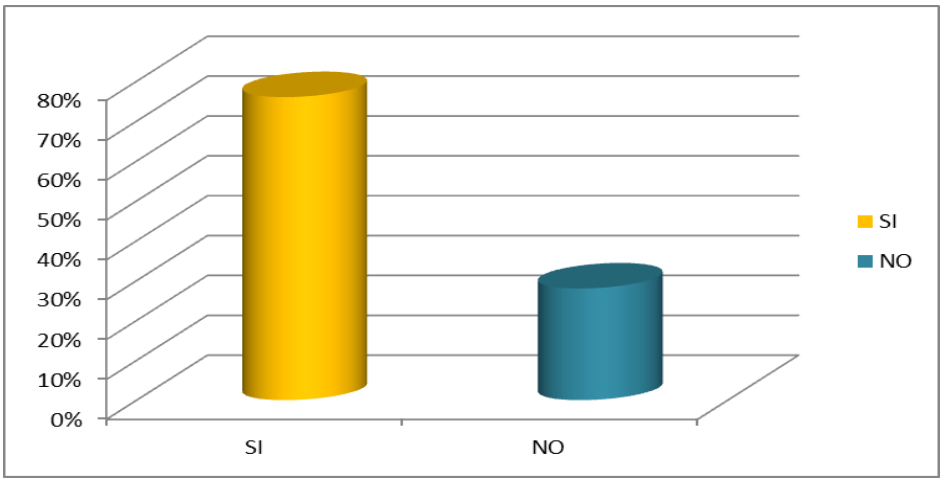
¿Considera necesario tomar medidas para sensibilizar al público, incluyendo a los usuarios del sistema educativo, del sistema legal y administración de justicia sobre la necesidad de prevenir y combatir el delito cibernético?

Tabla VII: Medidas para sensibilizar al público sobre la necesidad de prevenir y combatir el delito cibernético. -

ALTERNATIVA DE RESPUESTA	RESPUESTA	FRECUENCIA
SI	36	76%
NO	14	28%
TOTAL	50	100%

Fuente: Tabla elaborada por equipo investigador

Grafico VII: Medidas para sensibilizar al público sobre la necesidad de prevenir y combatir el delito cibernético. -



Fuente: Gráfico elaborado por equipo investigador

Interpretación de resultados: A la interrogante de que si se considera necesario tomar medidas para sensibilizar al público, incluyendo a los usuarios del sistema educativo, del sistema legal y administración de justicia sobre la necesidad de prevenir y combatir el delito cibernético el 76% respondió positivamente, mientras que le 34% dijo que no. Esto permite tener claridad sobre la poca concientización que hay en la población sobre como se puede evitar cometer el delito de hurto de identidad o como impedir ser victima de ella.

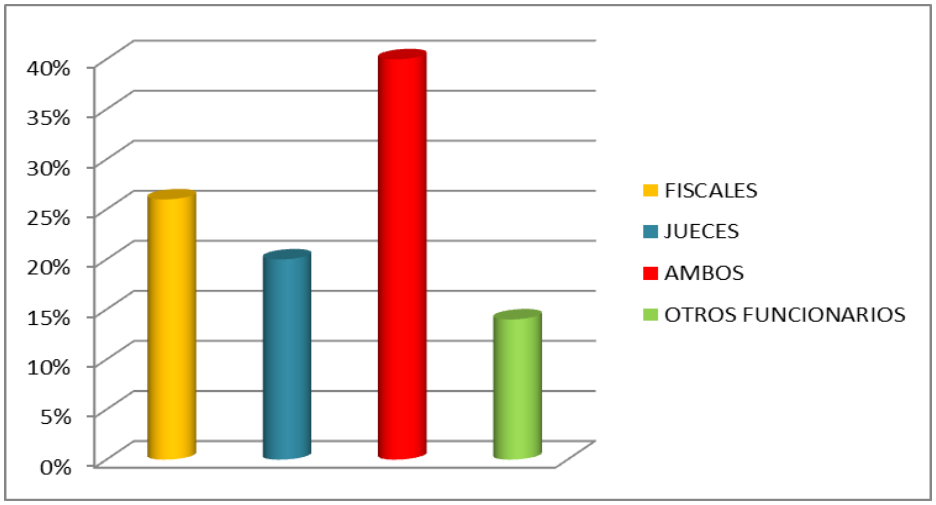
¿A cuáles funcionarios públicos considera que el Estado deberían orientar, de manera prioritaria, los programas de capacitación en materia de delito cibernético?

Tabla VIII: Funcionarios públicos a los que el Estado considera se deberían orientar, de manera prioritaria, los programas de capacitación en materia de delito cibernético.-

ALTERNATIVA DE RESPUESTA	RESPUESTA	FRECUENCIA
FISCALES	13	26%
JUECES	10	20%
AMBOS	20	40%
OTROS FUNCIONARIOS	7	14%
TOTAL	50	100%

Fuente: Tabla elaborada por equipo investigador

Grafica VIII: Funcionarios públicos a los que el Estado considera se deberían orientar, de manera prioritaria, los programas de capacitación en materia de delito cibernético.-



Fuente: Gráfico elaborado por equipo investigador

Interpretación de resultados: sobre, cuáles funcionarios públicos considera que el Estado debería orientar, de manera prioritaria, los programas de capacitación en materia de delito cibernético, respondieron de la siguiente manera, el 26% dijo que los fiscales, el 20% que los jueces, el 40% respondió que ambos y el 14%, que a otros.

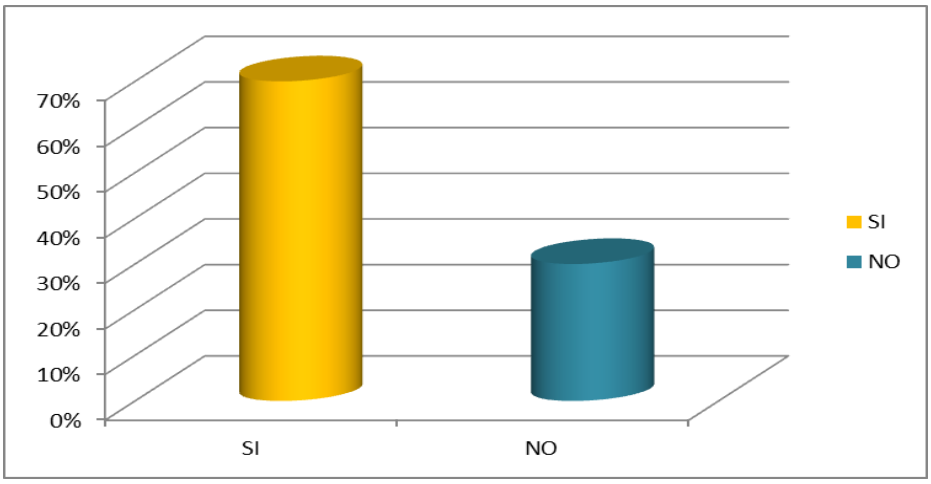
¿Ha identificado necesidades que tiene en materia de asistencia técnica y capacitación de funcionarios en delito cibernético?

Tabla IX: Necesidades que tiene en materia de asistencia técnica y capacitación de funcionarios en delito cibernético.-

ALTERNATIVA DE RESPUESTA	RESPUESTA	FRECUENCIA
SI	35	70%
NO	15	30%
TOTAL	50	100%

Fuente: Tabla elaborada por equipo investigador

Grafica IX: Necesidades que tiene en materia de asistencia técnica y capacitación de funcionarios en delito cibernético.-



Fuente: Gráfico elaborado por equipo investigador

Interpretación de resultados: en esta pregunta resulto que en el 70% de las respuestas que se obtuvieron se han identificado necesidades que se tiene en materia de asistencia técnica y capacitación de funcionarios en delito cibernético y el 30% dijo no haber identificado sobre lo antes dicho, esta se valora desde un punto de vista en el que la tecnología es pionera en tema de cometimiento de muchos delitos, por lo tanto es necesario actualizar y capacitar a todos los involucrados en el sistema de justicia en El Salvador.-

ANALISIS DE ENTREVISTAS.

En aras de dar cumplimiento al Objetivo Especifico II se realizaron entrevistas estructuradas, las cuales fueron dirigidas a especialistas en la materia, quienes dan respuesta penal a la acción delictiva investigada, así como a la diversidad de victimas involucradas en la ejecución del ilícito, indagando con ello la percepción de las debilidades que presenta nuestro sistema en relación al tipo que se estudia.

OBJETIVO ESPECIFICO II Analizar las debilidades que presenta el sistema jurídico en el tipo de delito de Hurto de Identidad.

PREGUNTAS DE LAS ENTREVISTAS REALIZADAS.

¿Sabe cuáles son los elementos típicos del delito de hurto de identidad que se deben reunir para configurarlo como tal?

De las personas entrevistadas fueron unánimes en establecer que dentro de los elementos típicos para que se configure el tipo es la suplantación o apoderamiento de la identidad de persona natural o jurídica, utilizando medios tecnológicos, una respuesta totalmente apegada a la disposición legal del delito de hurto de identidad.

¿Cuál o cuáles son los bienes jurídicos que protege el delito de hurto de identidad en la Ley Especial de Delitos Informáticos y conexos?

Las respuestas vertidas por los entrevistados consideran que los Bienes Jurídicos protegidos que consideran más susceptibles de vulneración son la identidad de la persona suplantada, el honor, la imagen de la misma, según el fin con el que se suplante la identidad de la persona.

¿Para usted, admite tentativa el delito de hurto de identidad y si es afirmativa porque?

La mayoría de los entrevistados consideraron que no admite el tipo penal la tentativa, ya que este se aprecia como un delito de mera actividad y no de resultado bastando que se consuma el delito con la mera suplantación de la identidad o el

apoderamiento de misma por medios de tecnologías, no pudiendo en consecuencias separarse espacio-temporalmente con la acción del resultado.

No obstante un porcentaje mínimo de entrevistados manifestaron que al ser un delito de resultado admite la tentativa.

¿Cuáles serian los problemas en las técnicas de investigación que implicaría acreditar autoría y participación del sujeto activo del delito de hurto de identidad?

Las respuestas que vertieron sobre los problemas en la técnicas de investigación en el delito hurto de identidad estipulan que los problemas que surgirían para acreditar la participación del sujeto activo vendrían derivados de los pocos recursos tecnológicos para individualizar a los responsables, así como la falta de disposición de la información de empresas que concentran los servicios de páginas Web, redes sociales entre otros.

¿Es preciso el artículo 22 de la Ley Especial de Delitos Informáticos y conexos, en delimitar la descripción típica del delito de hurto de identidad? ¿Por qué?

Las personas entrevistadas determinaron que el art. 22 LEDIC no es preciso, dado que no reúne las exigencias del principio de taxatividad, al no regular los elementos subjetivos del tipo, pero su precisión debe ser procedente, tomando en cuenta el principio de legalidad en que tiene que regirse toda conducta típica, la cual debe describirse con bastante exactitud.

¿Es un delito independiente o dependiente el delito de hurto de identidad regulado en el Art. 22 de la Ley Especial de Delitos Informáticos y conexos, con el delito hurto básico que regula el art. 207 del Código Penal? ¿Cuáles serian las diferencias esenciales?

La población entrevistada considero que ambos delitos son independientes si valoramos que protegen bienes jurídicos diferentes, como consecuencia de ello el delito de hurto básico se enfoca en proteger el patrimonio económico de las personas a diferencia del hurto de identidad que protege la identidad, imagen y honor de la victima radicando en la suplantación o apoderamiento, no sustrayéndola de quien pertenece si no un servidor de sistemas tecnológicos, según la manera en que se use la suplantación por lo que requiere también de técnicas investigativas diferentes.

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

A continuación se presentan las conclusiones y recomendaciones generadas en la investigación de campo que se realizo en la zona oriental sobre el delito de hurto de identidad, regulado en el art. 22 de la Ley Especial de Delitos Informáticos y Conexos, cuyo objetivo es que estas sean valoradas y así crear herramientas para enfrentar las consecuencias negativas que provocan los avances tecnológicos, en el cometimiento de hechos delictivos como el hurto de identidad, buscándose una solución que propicie el derecho a la identidad e intimidad de la persona.

5.1 CONCLUSIONES

- ✓ La criminalidad informática organizada ha crecido de manera exponencial, con incidentes altos de seguridad, vulnerabilidades, y los altos costos que involucran para las empresas o personas jurídicas, riesgos que son aprovechadas por los intrusos, ya que estos conocen cada vez con más profundidad los detalles de las tecnologías y sus limitaciones, siendo necesario capacitar al sistema penal sobre cómo evitar que estos puedan desaparecer la evidencia y confundir a los investigadores, siendo un reto para los sectores afectados, los legisladores, judiciales, policiales e incluso los especialistas informáticos encargados de su investigación.

- ✓ La criminalística al ser multidisciplinaria se aplica en temas de balística, medicina forense, física, química, e incluso la informática, entre otras, debe ser el apoyo del sistema judicial por medio de métodos y técnicas propias del trabajo de las diferentes disciplinas.

- ✓ Es necesario conocer el comportamiento de cómo los incidentes de seguridad, las vulnerabilidades y la criminalidad informática, es vital para el análisis de los delitos informáticos, ya que han tenido un repunte a lo largo de los últimos años, por ello, se requiere analizar la tendencia de dichos componentes.

- ✓ En nuestro país actualmente no se cuenta con una unidad especial dentro de la Fiscalía General de la Republica lo cual es necesario para evitar e investigar los delitos informáticos para impedir vulneraciones a los derechos de las personas y hacer justica en toda situación legal, en virtud de ello no se cuenta en tal institución con la infraestructura, herramientas y conocimientos técnicos suficientes para lograr los resultados necesarios para evitar la impunidad de tales delitos.

- ✓ El delito de Hurto de Identidad requiere hacer un diagnóstico de la actividad delictiva vinculada a las computadoras y la información, o que utiliza las computadoras como medio para cometer un delito; así como de la legislación, las políticas y las prácticas nacionales con respecto a dicha actividad.

- ✓ Se logro identificar que las instituciones (Juzgados comunes, Juzgados especializados, Fiscalía General de la Republica, Procuraduría General de la Republica, Policía Nacional Civil) encargadas de combatir los delitos, como las llamadas infracciones informáticas, no cuentan con la preparación y herramientas de orden técnico, y perseguir así tipos como el hurto de identidad, por la falta de una infraestructura necesaria, como centros de vigilancia computarizados e implementos tecnológicos.

- ✓ Ante los avances tecnológicos y las nuevas conductas delictivas es obligatorio fortalecer y desarrollar la cooperación internacional en áreas de especial preocupación tales como, la lucha contra el terrorismo, el combate contra la corrupción, el lavado de dinero, el narcotráfico, el fraude documentario, el tráfico ilícito de armas, el crimen organizado y la delincuencia transnacional, las cuales pueden ser cometidos utilizando los medios de la informática

5.2 RECOMENDACIONES

- ✓ Para dar una respuesta penal, a las nuevas formas de delinquir es necesario contar no solo con leyes e instrumentos eficaces y compatibles, sino, también con las infraestructuras, tanto técnicas como con el recurso humano calificado, para hacerle frente a este nuevo tipo de delito y cumplir con ello con la obligación jurídica en acatamiento de su mandato constitucional y combatir así esta clase de criminalidad a fin de precautelar los derechos de las victimas y llevar los responsables a juicio, ya que muchas veces estas conductas delictivas no son tratadas en forma debida por los entes obligados a su investigación y persecución.

- ✓ Ante estas nuevas figuras delictivas de avanzada tecnología que se cometen internacionalmente y de manera clandestina, es necesario capacitar a las partes del sistema judicial a fin de estudiar, explicar y predecir el cómo, dónde, cuándo, quién o quienes los cometen.

- ✓ Es necesario el fortalecimiento y capacitación de las instituciones encargadas de la persecución del delito de hurto de identidad, ya que la Fiscalía General de la República es la encargada de la parte acusatoria y de la búsqueda de pruebas incriminatorias.

- ✓ Se requiere una reforma o modificación en el sistema financiero, el cual prohíba a estas empresas compartir o proporcionar las condiciones financieras o crediticias de las personas beneficiadas por este sistema, así como la información personal de las mismas.-

- ✓ Es necesario generar o contar con un sistema de control informático eficiente en las instituciones públicas que cuentan con registros personales de los salvadoreños, a fin de, por un lado, no proporcionar información o datos personales que administran, a ciudadanos ajenos y sin autorización del sujeto a quien corresponde el derecho; así como evitar la intrusión informática ilegal de personas ajenas a la institución o al titular del derecho a tales sistemas, que tengan como objetivo sustraer esa información para su uso ilegal, por ejemplo, mediante la suplantación o apoderamiento de la identidad de tales personas.-

- ✓ Que se formen unidades investigativas integrales (Ministerio Publico Fiscal Especializado y agentes de la Policía Nacional Civil), que se les dote con los recursos tecnológicos necesarios (acceso permanente a internet, equipos, programas o software especializado en la pericia forense digital) y el recurso humano capacitado (en el uso de los equipos y programas especializados, así como en derecho penal informático), para abordar cuestiones de delincuencia cibernética, nacional y transnacional.

- ✓ Analizar los presupuestos institucionales de Fiscalía General de la República y Policía Nacional Civil, particularmente en la División de Policía Técnica y Científica, para programar los recursos financieros necesarios para cumplir con la recomendación anterior.

- ✓ Crear y difundir una política de concientización para la población en general, sobre el buen uso de las redes sociales, previniendo que la información brinda en dichas redes, los expone a ser victimas de una serie de delitos que les puede ocasionar daños, en su seguridad jurídica, patrimonio, imagen y otros.

GLOSARIO

- **ACTIVO PATRIMONIAL**: Conjunto de bienes y derechos que integran el haber de una persona física o jurídica.
- **BASE DE DATOS**: Conjunto completo de ficheros informáticos que reúnen informaciones generales o temáticas, que generalmente están a disposición de numerosos usuarios.
- **CIBERTERRORISMO**: Uso de un medio electrónico con el fin de causar terror en una población con fines políticos, económicos o religiosos. CORREO ADJUNTO: Archivos anexos enviados junto a un correo electrónico, suelen ser una forma común de propagación de virus de computadora.
- **COOKIE**: Es un archivo o datos dejados en su computadora por un servidor u otro sistema al que se hayan conectado. Se suelen usar para que el servidor registre información sobre aquellas pantallas que usted ha visto y de la información personalizada que usted haya mandado. Muchos usuarios consideran esto como una invasión de privacidad, ya que casi ningún sistema dice lo que esta haciendo. Hay una variedad de "anti-cookie" software que automáticamente borra esa información entre visitas a su sitio.
- **CRACKER:** Personas que se dedican a explotar las vulnerabilidades de un sistema con fines maliciosos.
- **DATOS PERSONALES:** Es cualquier información relacionada con el usuario, por ejemplo, el nombre, teléfono, domicilio, fotografía o huellas dactilares, así como cualquier otro dato que pueda servir para identificar. Este tipo de datos te permiten además, interactuar con otras personas, o con una o más organizaciones. DELITO INFORMÁTICO: Delito cometido utilizando una computadora; también se entiende por delito informático cualquier ataque contra un sistema computarizado.
- **DAÑO:** Perjuicio, mal o desgracia.
- **DELITO**: Acción u omisión voluntaria o imprudente penada por la ley.

- **FIRMA DIGITAL:** El equivalente digital de una firma autentica escrita a mano. Es un dato añadido a un fichero electrónico, diciendo que el dueño de esa firma escribió o autorizo el Archivo.

- **FRAUDE INFORMÁTICO**. La incorrecta utilización del resultado de un procesamiento automatizado de datos, mediante la alteración en cualquiera de las fases de su procesamiento o tratamiento informático, siempre que sea con ánimo de lucro y en perjuicio de tercero.

- **HACKER:** Persona que accede a un sistema informático sin autorización para ver su funcionamiento interno y explotar vulnerabilidades.

- **HURTO DE IDENTIDAD:** o **robo de identidad** ó **usurpación de identidad** es la apropiación de la identidad de una persona: hacerse pasar por esa persona, asumir su identidad ante otras personas en público o en privado, en general para acceder a ciertos recursos o la obtención de créditos y otros beneficios en nombre de esa persona.

- **IDENTIDAD**: Es un **conjunto de características** propias de una persona o un grupo y que permiten distinguirlos del resto. Se puede entender también como la **concepción** que tiene una persona o un colectivo sobre sí mismo en relación a otros.

- **INFORMÁTICA:** Conjunto de conocimientos científicos y técnicos que hacen posible el tratamiento informático de la información por medio de ordenadores.

- **NAVEGADOR WEB:** Aplicación que opera a través de Internet, interpretando la información de archivos y sitios web para que podamos ser capaces de leerla. El navegador interpreta el código, HTML generalmente, en el que está escrita la página web y lo presenta en pantalla permitiendo al usuario interactuar con su contenido y navegar hacia otros lugares de la red mediante enlaces o hipervínculos

- **PHARMING**: Variante de Phishing que consiste en suplantar el sistema de resolución de nombres de dominio (DNS) para conducir al usuario a una página web falsa. PHISHING: Técnica de la Ingeniería Social que consiste en la suplantación de sitios de Internet, se puede presentar en correos electrónicos y

páginas web fraudulentas que aparentan proceder de instituciones de confianza como bancos o instituciones públicas.

- **PROTECCION JURIDICA**: es una garantía por la cual se cubren los gastos de un asegurado como consecuencia de su intervención en un procedimiento administrativo, arbitral o judicial, en el ámbito de la vida particular.

- **RED SOCIAL:** Sistemas o estructuras sociales en los que se realiza un intercambio entre sus miembros, y de los miembros de una red con los de otra, que puede ser otro grupo u otra organización. Esta comunicación dinámica permite sacar un mejor provecho de los recursos que poseen los miembros de estas redes. Los individuos o miembros son llamados “actores” o “nodos” en las publicaciones que detallan el funcionamiento de las redes sociales, y se llama “aristas” a las relaciones entre ellos. Las relaciones entre los miembros de las redes sociales pueden girar en torno a un sin número de situaciones tales como el intercambio de información, el financiero, o simplemente la amistad o las relaciones amorosas.

- **REPARACION CIVIL**: Resarcimiento del bien o indemnización por quién produjo el daño delictivo, cuando el hecho afectó los intereses particulares de la víctima

- **RESARCIR**: Dar una cosa o hacer un beneficio a una persona como reparación de un daño, perjuicio o molestia que se le ha causado.

- **SABOTAJE INFORMÁTICO**: Conducta ésta que va dirigida esencialmente a menoscabar la integridad y disponibilidad de la información.

- **SEGURIDAD INFORMÁTICA:** Área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con está implementando una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información.

- **SKIMMING:** Esta práctica es conocida también como clonación de tarjetas de crédito o débito, consiste en la duplicación de tarjetas de crédito o débito sin el consentimiento del dueño de la tarjeta.

- **SPEAR PHISHING:** Variante del Phishing tradicional destinada a conseguir datos de toda una organización o de un grupo de personas.
- **VICTIMA**: Persona que sufre un daño o un perjuicio a causa de determinada acción o suceso.

BIBLIOGRAFÍA.

Libros:

- Arango Durling, Virginia. (2001). El iter criminis. Editorial Panamá Viejo, Primera Edición, Panamá.
- Asamblea Legislativa, Senado de Puerto Rico (2009), Informe Negativo, sobre el P. del S, Segunda Sesión Ordinaria 16ta. 4 de noviembre de 2009. Pág. 2.
- Cabana, Patricia Faraldo, (2010) Suplantación de identidad y uso de nombre supuesto en el comercio tradicional y electrónico; Revista De Derecho Penal y Criminología, 3.a Época, N° 3, Coruña, España.
- Carlos Alberto Cerda Aceved. (2016). Características del Derecho Internacional Penal y su clasificación entre Crimen y Simple Delito. Editora Working paper N° 64 Programa Derecho Internacional. Valparaíso, Chile.
- Castellanos Hernández, Eduardo de Jesús. (2011). *El derecho a la identidad como derecho humanos*. Primera edición, Editorial Bucareli No. 99, México.
- Choclán Montalvo, J. A. (2001). Fraude informático y estafa por computación. Een CDJ, núm. 10, España.
- Coz Hernández, José Ramón, (2010). Modelo de madurez para la privacidad de una red social virtual; Editorial Liz, Madrid, España.
- De Salvador, Carrasco Luis. (2010), Casos de suplantación de identidad detectados en denuncias tramitadas por la Agencia Española de Protección de Datos. Ed. Arazandi-Thomson Reuters-Agencia Española de Protección de Datos-Universidad de Castilla-La Mancha. Pamplona, España.
- Delgado Martin, José María. (2009). La criminalidad organizada. Editorial J.M. Bosch, Barcelona, España.
- Faraldo Cabana, Patricia. (2011). Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico. Editorial Liz, Valencia, España.
- Fernández Priego, Verónica. (2014). La protección y seguridad de la persona en internet: Aspectos sociales y jurídicos. Primera edición, Editorial Reus S.A., Madrid, España. Pág. 52.
- Gabaldón, Luis Gerardo, (2008) Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico. Editorial Sociologías, Porto Alegre, Brasil, Nº 20.

- Gercke, Marco. (2013). Manual sobre los delitos relacionados con la identidad. Oficina de las Naciones Unidas contra la Droga y el Delito. Naciones Unidas, Nueva York, 2013. Pág. 07.
- González de la Vega, Francisco, (1998). Derecho penal mexicano, los delitos en general. Vigésima cuarta edición. México, Editorial Porrúa.
- Gutiérrez Francés, María Luz. (2011). Notos sobre la delincuencia informática: atentados contra le información como valor económico de la empresa. Editorial San Marcos, Lima, Perú.
- Hernández M., Alma Rosa; Rodríguez Cortés, Karina, (2011). La organización para la cooperación y el desarrollo económico, OCDE, y la definición de competencias en educación superior. Editorial Educere, vol. 12, núm. 43.
- Herrera Moreno, Miriam. (2001). El fraude informático en Derecho penal español. Editorial Arasendi, núm. 39, España.
- Jareño, Leal Ángeles. (2012). Intimidad e imagen, los límites de la protección penal. Editorial Iustel, Madrid, España.
- López Vázquez, Delfino (2013). La suplantación de identidad de tipo físico, informático y de telecomunicaciones como nueva manifestación de las conductas antisociales. Revista Colectivo Arcion, visión criminológica-criminalística, Puebla, México. Pág. 07.
- Loredo González, Jesús Alberto. (2013). Delitos informáticos: su clasificación y una visión general de las medidas de acción para combatirlo. Editorial FCFM-UANL, Facultad de Ciencias Físico Matemáticas Universidad Autónoma de Nuevo León San Nicolás de los Garza, Nuevo León, México. Pág. 45.
- Mata y Martin, Ricardo. (2010). El robo de identidad: ¿una figura necesaria? en robo de identidad y protección de datos. Ed. Arazandi-Thomson Reuters-Agencia Española de Protección de Datos-Universidad de Castilla-La Mancha, Pamplona, España.
- Matute, Sergio. (2012), Los Sistemas de Información, La Informática Jurídica, y el sistema UNAN JURE. Segunda Edición, Editorial UNAM Jurídica, México, Pág. 107.
- Miró Llinares, Fernando. (2014). La oportunidad criminal en el ciberespacio. Aplicación y desarrollo de la Teoría de las actividades cotidianas para la prevención del cibercrimen". Editorial RECPC, núm. 13-07, España.

- Ortega Giménez, Alfonso. (2015). *La Regulación de Internet*. Revista de Derecho Informático Alfa-Redi. Núm. 061, Argentina.
- Pérez Ángeles, Juan Manuel. (2013). El criminólogo-criminalista ante el fenómeno delictivo. Año 1 Número1, Enero-Marzo 2013. Colectivo Arcion. Puebla, México. Pág. 11.
- Plascencia Villanueva, Raúl. (2004). Teoría del Delito. Instituto de Investigaciones Jurídicas, Estudios doctrinales Numero 192, Tercera reimpresión, Universidad Autónoma de México.
- Rebollo Delgado, Lucrecio. (2012). El derecho a la protección de datos en España y Argentina orígenes y revolución vigente. Editorial Dykinson, Madrid, España.
- Rodríguez Bernal, Antonio Pedro. (2011). Los cibercrímenes en el espacio de libertad, seguridad y justicia. Revista de Derecho Informático, núm. 103, Madrid, España.
- Romeo Casabona, Carlos María. (2007). *De los delitos informáticos al cibercrimen*. Ediciones universitarias de Salamanca, Primera edición, España.
- Romero Flores, Rodolfo, (2014). Las conductas vinculadas a la suplantación de identidad por medios telemáticos: una propuesta de acción legislativa. Editorial Investigaciones Jurídicas, Unam, México.
- Romero Flores, Rodolfo. (2016). La conductas vinculadas a la suplantación de identidad por medios telemáticos: una propuesta de acción legislativa. Editorial Unam, México.
- Sampedro, José Luis (2002). *Técnica y Globalización*. Boletín Económico de ICE, Nº 2750, España.
- Tamayo Tamayo, Mario. (2004). Diccionario de la investigación científica, 2da Edición, editorial LIMUSA, México.
- Téllez Valdés, Julio (2003). Derecho Informático. 3ª edición, Editorial McGraw Hill Serie Jurídica, México. Pág. 285.
- Teruelo, J.G. (2014). Derecho penal e Internet. Especial consideración de los delitos que afectan a jóvenes y adolescentes. Editorial Lex Nova, Valladolid, España.
- Zorrilla, Santiago, (2014). Metodología de la Investigación, editorial McGraw-Hill. 5ª Edición, Madrid, España.

Enlaces web:

- ww.gpfmln.sv. (08 de febrero de 2016). http://www.gpfmln.sv. Recuperado el 22 de marzo de 2017, de http://www.gpfmln.sv/index.php/2-prensa/sesion-plenaria/1093-08021602.
- Asamblea.gob.sv. (18 de agosto de 2015). http://www.asamblea.gob.sv. Recuperado el 21 de marzo de 2017, de http://www.asamblea.gob.sv/noticias/archivo-de-noticias/retoman-estudio-de-ley-contra-delitos-informaticos.

ANEXOS

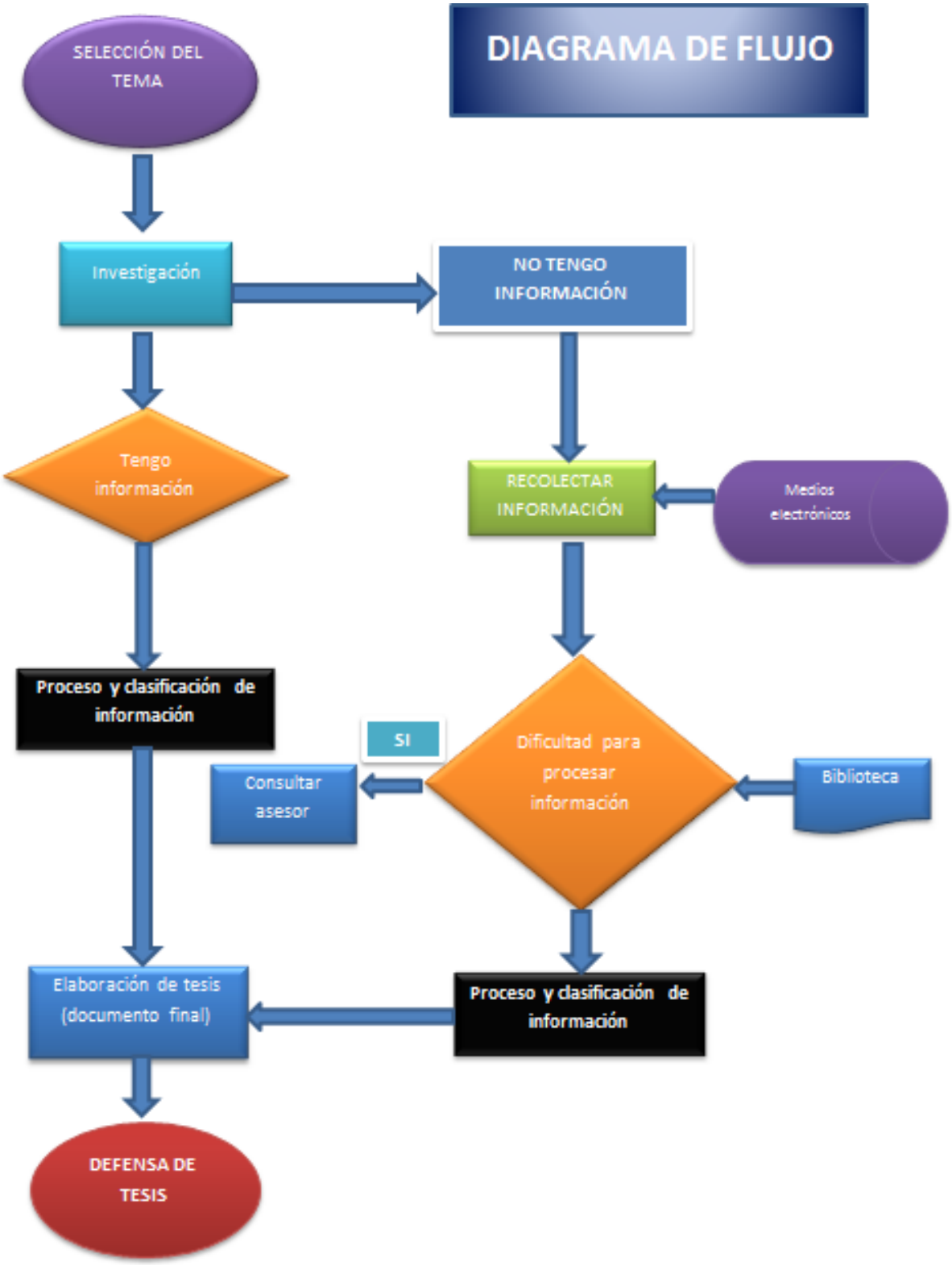


DIAGRAMA DE FLUJO
SELECCIÓN DEL TEMA
Investigación
NO TENGO INFORMACIÓN
Tengo información
RECOLECTAR INFORMACIÓN
Medios electrónicos
Proceso y clasificación de información
SI
Dificultad para procesar información
Consultar asesor
Biblioteca
Elaboración de tesis (documento final)
Proceso y clasificación de información
DEFENSA DE TESIS

ANEXO Nº 1

UNIVERSIDAD GERARDO BARRIOS

FACULTAD DE POSTGRADO

MAESTRÍA EN DERECHO PENAL

TEMA: “Los efectos jurídicos e incidencia del delito de Hurto de Identidad en la Ley Especial de Delitos Informático y conexos en la zona oriental”.

GUÍA DE ANÁLISIS JURISPRUDENCIAL

Identificación Jurisprudencial

Nombre del procesado: _____

Nombre del perjudicado: _____

Sala o Cámara: _____

Lugar: _____

Identificación de la sentencia: _____

Fecha: ___ / ____ / ____

Tema de análisis preferentes o descriptores: _____

_____

Resolución Originaria o Recurrida:

 Tipo de acción o recurso:

_____

 Motivo del Recurso:

_____

_____

_____

_____

Investigados

 Hechos Acusados

Probados

 Normativa Vinculada:

_____

_____

 Lineamientos Arguméntales:

_____

_____

Actor (tesis recursiva):

_____

_____

_____

Contraparte (antítesis):

_____

_____

_____

 Clase de interpretación por Cámara o Sala:

_____

_____

_____

 Doctrina Legal (síntesis):

_____

_____

_____

_____

 Problema jurídico:

_____

_____

 Decisión:

_____

_____

 Fundamento de la decisión:

_____

_____

Precedentes a considerar:

_____

_____

Decisiones posteriores a considerar:

_____

_____

Voto disidente (si lo hubiera):

_____

Análisis:

_____

_____

Dogmática aplicada:

_____

_____

Temas desarrollados y relacionados con la intervención corporal y vulneración a derechos fundamentales:

_____

_____

_____

Comentarios y conclusiones (síntesis):

_____

_____

ANEXO N°2

UNIVERSIDAD GERARDO BARRIOS

FACULTAD DE POSTGRADO

MAESTRÍA EN DERECHO PENAL

TEMA; Los efectos jurídicos e incidencia del delito de hurto de identidad en la Ley Especial de Delitos Informáticos y conexos en la zona oriental.

OBJETIVO: Investigar los conocimientos que poseen los encuestados sobre el delito de hurto de identidad y los problemas interpretativos de diversas modalidades.

INDICACIONES: Conteste según su saber y entender, de acuerdo a los conocimientos que la práctica judicial le ha impartido.

1. ¿Sabe cuáles son los elementos típicos del delito de hurto de identidad que se deben reunir para configurarlo como tal?

2. ¿Cuál o cuáles son los bienes jurídicos que protege el delito de hurto de identidad en la Ley Especial de Delitos Informáticos y conexos?

3. ¿Para usted admite tentativa el delito de hurto de identidad y si es afirmativa porque?

4. ¿Cuáles serian los problemas en las técnicas de investigación que implicaría acreditar autoría y participación del sujeto activo del delito de hurto de identidad?

5. ¿Es preciso el artículo 22 de la Ley Especial de Delitos Informáticos y conexos, en delimitar la descripción típica del delito de hurto de identidad? ¿Por qué?

6. ¿Es un delito independiente o dependiente el delito de hurto de identidad regulado en el Art. 22 de la Ley Especial de Delitos Informáticos y conexos, con el delito hurto básico que regula el art. 207 del Código Penal? ¿Cuáles serian las diferencias esenciales?