ANÁLISIS DOCUMENTAL DEL DELITO HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES ARTÍCULO 269I (LEY 1273/2009) EN CÚCUTA

WILLIAM HERNEY ARIZA SALCEDO
LUIS GERARDO RODRIGUEZ HARO
MARIO ADUL VILLAMIZAR DURAN

UNIVERSIDAD SIMÓN BOLÍVAR SEDE CÚCUTA
FACULTAD DE CIENCIAS JURÍDICAS SOCIALES
PROGRAMA ACADÉMICO DE DERECHO
SAN JOSE DE CUCUTA
2018-2

ANÁLISIS DOCUMENTAL DEL DELITO HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES ARTÍCULO 269I(LEY 1273/2009) EN CÚCUTA

WILLIAM HERNEY ARIZA SALCEDO
LUIS GERARDO RODRIGUEZ HARO
MARIO ADUL VILLAMIZAR DURAN

Proyecto de Trabajo de investigación presentado como prerrequisito para optar título de Abogado

Docente
ANDREA AGUILAR BARRETO
Doctora

UNIVERSIDAD SIMÓN BOLÍVAR SEDE CÚCUTA
FACULTAD DE CIENCIAS JURÍDICAS SOCIALES
PROGRAMA ACADÉMICO DE DERECHO
SAN JOSE DE CUCUTA
2018-2

Tabla de contenido

Lista De Anexos

Titulo

ANÁLISIS DOCUMENTAL DEL DELITO HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES ARTÍCULO 269I (LEY 1273/2009) EN CÚCUTA

Introducción

La presente investigación está motivada por el continuo incremento de conductas delictivas cometidas a través de dispositivos informáticos, los cuales son todos aquellos aparatos tecnológicos que permiten ejecutar tareas desde la red facilitando la vida cotidiana de las personas, entre otras cosas dichos dispositivos están siendo utilizados para atentar contra el patrimonio de los usuarios de transacciones bancarias en Cúcuta , una transacción bancaria hace referencia a cualquier tipo de operación de dinero en la cual interviene el banco, como por ejemplo el pago con una Tarjeta de Crédito o Débito, retiro de fondos desde la Cuenta Corriente, cambio de cheques, transferencias de dinero, giros desde un cajero automático, entre otras.

Cabe resaltar que la evolución del ciberdelito, como lo afirma SEOtop (2015), permite considerar los ciberdelitos como:

"Actos criminales que implican el uso de ordenadores o de internet. Por ejemplo, los crímenes de odio en redes sociales, el telemarketing y el fraude en Internet, el robo de identidad, y de la cuenta de tarjeta de crédito son considerados como delitos cibernéticos o ciberdelitos."

A nivel internacional esta problemática es considerada como lo afirma Miró (2012):

"Un fenómeno de la criminalidad relacionada con el uso de las Tecnologías de la Información y la Comunicación (en adelante TIC) sigue siendo totalmente novedoso y por ello, parcialmente incomprendido por la sociedad en general y, en particular, por las

instituciones que tienen que afrontar la prevención de esta amenaza. El cibercriminal forma parte ya de la realidad criminológica de nuestro mundo.”

En nuestro contexto ha contrastado con la involución de leyes, doctrina e incluso jurisprudencia referente a los delitos informáticos, este orden se encuentra bífido con un extremo en el que los delincuentes aprovechan los avances tecnológicos para hurtar y apoderarse de bases de datos que logran vulnerar la seguridad de los usuarios del sistema financiero colocando a estos a merced de la vulneración a su información (privada, personal, bancaria, secreta, empresarial, etc.); en el otro extremo se encuentra la paralización y atraso del marco jurídico de los delitos informáticos en Colombia unido a la desproporcionada incapacidad de los administradores de justicia y juristas que no logran blindar a las personas frente al cyberdelito y en el evento cuándo se produce la afectación a los usuarios no se consigue la reparación a estos y la obtención de justicia es en la mayoría de los casos nula.

Problema

Planteamiento del Problema

En Colombia en el año 2009, el congreso de la república promulgó una ley, la 1273 "Por medio del cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "De la Protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones". En aras de brindar un mecanismo de protección para las personas que fueran víctimas de delitos a través de medios informáticos, puesto que en el país no se contaba con ningún tipo de mecanismo para tratar estos delitos como tal.

Como estudiantes de derecho realizaremos un análisis documental de dicho artículo para determinar si es eficiente en lo referente a combatir los delitos cometidos a través de los diferentes medios informáticos y semejantes, y sin recibir alguna modificación o adecuación de los tipos penales en el tiempo que lleva de vigencia dicho artículo, ¿se puede adelantar un proceso penal mediante este artículo?, teniendo en cuenta que los sujetos que cometen estos tipos de delitos cada vez más van evolucionando en su actuar y con el auge de nuevas tecnologías han logrado llevar a cabo sus intenciones y al ver que la ley es "ineficaz" se han salido con la suya.

Formulación del Problema

¿El análisis del artículo 269i de la ley 1273 de 2009 ayudará para plantear soluciones frente a los delitos informáticos en Cúcuta, determinando los vacíos de la ley en Colombia?

Objetivos

Objetivo general

Identificar los vacíos existentes tras el análisis del artículo 269i de la ley 1273 de 2009 en el área metropolitana de Cúcuta frente a la legislación internacional y la adecuada tipificación de los delitos informáticos que contribuya a formular propuestas efectivas para combatir los delitos informáticos.

Objetivos específicos

Realizar un análisis documental del artículo 269i, hurto por medios informáticos y semejantes frente al actual marco legislativo internacional y la ley 1273 en Colombia.

Consultar la legislación contra los delitos informáticos de las legislaciones en Argentina, Venezuela y Chile realizando un comparativo con la Ley 1273 de 2009 para determinar las falencias en Cúcuta.

Crear una guía en donde se evidencian propuestas puntuales que contribuyan a mejorar la protección de datos actual frente a la ley 1273 de 2009 en Cúcuta.

Justificación

La importante y real evolución tecnológica a nivel mundial ha traído consigo un nuevo fenómeno llamado cibercrimen, que según lo afirma Rayón y Gómez (2014):

"Es cualquier infracción punible, ya sea delito o falta, en el que se involucra un equipo informático o Internet y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito que se ha desarrollado y ha crecido a pasos agigantados con una constante innovación en conductas punibles que dan como resultado la afectación de los usuarios de internet y medios informáticos."

Esta investigación está desarrollada con el propósito de establecer el punto en que nos encontramos frente a la lucha del hurto por medios informáticos Artículo 269I: Hurto por medios informáticos y semejantes (Ley 1273 de 2009) y así argumentar jurídicamente el manejo que debe darse a esta problemática, mediante el conocimiento veraz de las personas que han sido víctimas de este delito en Cúcuta, logrando crear una acción real entre las normas existentes, la correcta aplicación e interpretación de los administradores de justicia y los usuarios de la red y los sistemas financieros en Cúcuta, para pugnar de manera frontal a los ciberdelincuentes en Cúcuta.

Marco Referencial

Antecedentes

En los estudios que se realizarán de los delitos informáticos en Colombia y en la aplicación de la ley que los penaliza (ley 1273 de 2009) debemos revisar y tener en cuenta los antecedentes que podamos encontrar sobre este fenómeno en el país, a fin de obtener un mejor análisis acerca de esta situación, para ellos debemos tener en cuenta fuentes confiables que nos permitan consultar y ver el avance que puede tener esta investigación.

El artículo de investigación denominado: aproximación al estudio de los delitos informáticos, publicado por Juan Carlos Prías Bernal Profesor de la Universidad Javeriana (Colombia). En este artículo explica un estudio que se realizó a las incidencias de las nuevas tecnologías y la aplicación en el derecho penal colombiano el cual arrojo que en las actividades tecnológicas utilizadas actualmente son cobijadas por la legislación penal colombiana, cabe resaltar que no todas las actividades son cobijadas ya que no se enmarcan dentro de la legislación penal debido a la tipificación que se les da en el código. Este artículo nos ayudara a identificar los vacíos legales que existen en la legislación penal acerca de los delitos informáticos.

El artículo de investigación denominado: análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación, presentado por Juan David Rodríguez Arbeláez en la Universidad CES (Colombia). Este artículo se enfoca en realizar un análisis acerca de los diferentes tipos de delitos informáticos que son cometidos en las diferentes redes sociales y deja en duda la actuación o articulación que tiene la presente ley para proteger a los usuarios de este tipo de red social. Este artículo de investigación nos ayudara en el proceso de

identificar la escasa tipificación de los delitos informáticos y la poca protección que hay contra estos en la legislación colombiana.

El ensayo jurídico denominado: el delito informático contra la intimidad y los datos de la persona en el derecho colombiano, publicado por Libardo Orlando Riascos Gómez de la Universidad de Nariño (Colombia). Este ensayo jurídico es un estudio socio jurídico el cual analiza de fondo la establecido en la legislación penal sobre el tema de los delitos informáticos en Colombia, así mismo hace una comparación con las leyes de otros países y nos demuestra cuales son las falencias de nuestra legislación acerca de este tema. Este ensayo nos guiara para realizar un análisis comparativo de las legislaciones de otro país con la nuestra.

El artículo de investigación denominado: caracterización de los delitos informáticos en Colombia, publicado por Iván Manjarrés Bolaño y Farid Jiménez Tarriba de la Corporación Universitaria Americana (Colombia). En dicho artículo se realiza un repaso de los delitos informáticos de manera general y después se realiza al plano más específico, enfocado en la legislación actual colombiana. Con este artículo podemos tener una base de los antecedentes de los delitos informáticos.

El proyecto de grado denominado: análisis comparativo sobre delitos informáticos en Colombia con relación a seis países de Latinoamérica, presentado por Andrés Bolaños Díaz y Teresa de Jesús Narváez Narváez en la Universidad Nacional abierta y a Distancia UNAD en la ciudad San Juan de Pasto (Colombia). En este proyecto de grado realizan una comparación entre la legislación de 6 países latinoamericanos y Colombia con relación a los delitos informáticos, así mismo hacen una comparación entre los marcos normativos de los diferentes países. Este proyecto nos ayudará para realizar un análisis entre la legislación colombiana y la de los demás países de américa latina.

El ensayo denominado: la práctica de delitos informáticos en Colombia, presentado por Edison Raúl Serrano Buitrago en la Universidad Militar Nueva Granada (Colombia). Este ensayo nos enseña los errores que cometen los usuarios ya que no saben manipular las diferentes herramientas informáticas, al no utilizarlas con precaución y explica la necesidad de la implementación de controles de seguridad los cuales deben adecuarse a las situaciones que presentes los diferentes usuarios. A si como la explicación a estos de las diferentes herramientas.

El proyecto de grado denominado: mitigación de riesgo de delitos informáticos en el contexto empresarial, presentado por Carlos Fernando Tovar Yepes y Kevin Amariles Bedoya en la Universidad Tecnológica de Pereira en la ciudad de Pereira- Risaralda (Colombia). En este proyecto nos explican qué tratamiento se les da a los delitos informáticos en Colombia especialmente en el contexto empresarial, lastimosamente la mayoría de estas no están listas para enfrentar este tipo de ataques. Este tipo de investigación nos ayudará para entender la vulnerabilidad que tienen las empresas frente a los delitos informáticos.

Marco Teórico

Delitos informáticos.

Desde hace varios años el tema del delito electrónico se empezó a trabajar, luego se le dio el nombre de delitos informáticos y hoy en día es un tema bastante consolidado debido al avance tecnológico, debido al surgimiento de la tecnología también ha surgido los ciberdelitos y con ello las personas están menos protegidas sobres sus datos personales, las empresas también están desprotegidas. Por ello se han creado la forma o mecanismos de control para evitar que dichos delitos sean cometidos y sancionar a las personas que los comenten. Varios teóricos o expertos

en informática y en derecho penal han opinado desde su punto de vista profesional sobre el concepto de delito informático y lo han definido así:

Según la Doctora María de la Luz Lima (1984) dice que el delito electrónico:

"En un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin. En este sentido, se puede observar que la delincuencia va mucho más allá de la comisión de un delito como tal de forma física, ya que se busca facilitar la materialización de los mismos mediante el uso de los recursos tecnológicos disponibles, es aquí donde la conceptualización del delito informático en forma típica y atípica surge como lo conceptualiza Julio Téllez Valdez 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."

Según el experto italiano Carlos Sarzana (1979) en su obra - Criminalita e tecnología, se define como delito informático a: "los crímenes por computadora comprenden cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo".

En el año 2001 en la ciudad de Budapest se llevó a cabo el primer congreso contra la cibercriminalidad, en este congreso delimitaron los tipos de delitos informáticos, en dicho proceso los países incluidos en la ONU intervinieron en esta creación, como culminación de este congreso se promulgo un tratado con el cual se busca tipificar y establecer las normas que van en contra de los delitos informáticos en el ámbito internacional y debe ser aplicado en cada país

miembro de la ONU. Para el análisis del presente proyecto se toma como base la clasificación realizada por ―Convenio de Ciberdelincuencia, firmado en Budapest el día 23 de noviembre de 2001 y el cual comenzó a regir a partir del 1 de julio de 2004. Este convenio agrupa de acuerdo a su definición y enfoque los delitos informáticos de la siguiente manera:

Titulo I - Delitos contra la confidencialidad, la integridad, y la disponibilidad de los datos y sistemas informáticos.

- Art. 2: Acceso ilícito
- Art. 3: Interceptación ilícita
- Art. 4: Ataques a la integridad de los datos
- Art. 5: Ataques a la integridad del sistema
- Art. 6: Abuso de los dispositivos

Titulo II - Delitos informáticos.

- Art. 7: Falsificación informática
- Art. 8: Fraude informático

Titulo III - Delitos relacionados con el contenido.

Art. 9: Delitos informáticos relacionados con la pornografía infantil

Titulo IV - Delitos relacionados con infracciones de la propiedad intelectual y derechos afines.

Art. 10: Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines (ONU, 2001).

El artículo 1 se omite de este proyecto ya que se refiere a las definiciones o términos.

La evolución de los delitos informáticos según el experto Ricardo Posada Maya:

"Cuando se habla de delitos informáticos y su origen, se debe tener claro que los delitos sean informáticos o no nacen, crecen y evolucionan. Desde los inicios de la informática con la creación del primer computador y la internet (en sus inicios ArpaNET) el hombre no imagino la importancia que tendría estos dos grandes avances, ya sea por la optimización de recursos en las actividades laborales y ahora cotidianas, se deja de hablar de largas distancias para contemplar la posibilidad de comunicarse en tan solo unos segundos con alguien que se encuentre al otro lado del mundo. Los delitos informáticos, ya no son los mismos de hace 10 o 20 años atrás, han evolucionado adaptándose a las nuevas tendencias del mercado tecnológico que cada vez crece más gracias al consumismo existente. Teniendo en cuenta estos aspectos se puede observar por ejemplo que en los años 70's con el auge de las computadoras en todo el mundo aparecieron los primeros delitos contra los sistemas informáticos como el espionaje, el sabotaje, manipulación y fraude en donde el delincuente buscaba lucrarse económicamente, por esta razón no se consideraban aún como delitos informáticos, sino como delitos comunes tipificados en los códigos penales de los diferentes países. A esto, suele sumarse las venganzas por funcionarios despedidos quienes causaban daños físicos como cortos circuitos, ataques de denegación de servicios (DDoS) entre otros. No obstante en los años 80's con la aparición de los ordenadores personales surge también los delitos como la piratería atacando de esta manera en forma un poco primitiva a la propiedad intelectual o derechos de autor, siendo este los inicios de una nueva fase de delitos que se forjan a través del uso de la informática y las telecomunicaciones."

Analizando lo dicho y entrando en la actualidad, a partir de los años 90's y a la fecha estos delitos han ido en aumento por ello han surgido nuevas maneras de tipificarlos en las

legislaciones nacionales para poder combatir este delito y sancionar a los responsables. A su vez se ha creado un marco internacional en el cual se han definido las características de estos delitos, especificando como son, como se materializan y que sanciones se les debe aplicar a los culpables de dicho delito.

Es así, como en Budapest el 23 de Noviembre de 2001 se firma el ―Convenio de Ciberdelincuencia, el cual comenzó a regir a partir del 1 de julio de 2004, el objetivo de esta es tener disposiciones legales frente al tratamiento y sanción de todas las acciones de la ciberdelinciencia, siendo este el primer marco legislativo que las naciones siguieron y aplicaron como parte de prevención de los delitos informáticos (ONU, 2001).

Delitos informáticos tipificados en Colombia.

En Colombia se creó el 5 de enero del año 2009 la ley 1273 en la cual se tipificaron los delitos informáticos los cuales se denotan de la siguiente forma: "acceso abusivo a un sistema informático. Es considerado como una intrusión a un sistema informático, violando toda seguridad implantada por el administrador del sistema o webmaster en su defecto, de acuerdo al Abogado y Especialista colombiano en derecho Ricardo Posada Maya, este delito se describe como: […] arrogarse ilegalmente ―de forma no autorizada―el derecho o la jurisdicción de intrusarse o „ingresar" en un sistema informático o red de comunicación electrónica de datos, con la consecuente trasgresión de las seguridades dispuestas por el "Webmaster" o prestador del servicio al "Webhosting" u "Owner", con el fin de proteger los servicios de transmisión, almacenamiento y procesamiento de datos que ofrece frente a posibles abusos de terceros (ingreso en cuentas de e-mail ajenas). Así como también la utilización o interferencia indebidos de dichos equipos o sistemas informáticos o telemáticos, o la permanencia contumaz en los

mismos por fuera de la autorización o del consentimiento válidamente emitido por el titular del derecho.

Colombia este delito se considera dentro del capitulo I de la ley 1273 de 2009, la cual lo cita como:

Artículo 269ª.

Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo […]

Este delito puede considerarse en su forma más básica como una denegación de servicio o ataque DDoS, el cual se define según la CERT como:

"Ataque caracterizado por un intento explícito de denegar a los usuarios legítimos el uso de un servicio o recurso."

Por lo que es clasificado dentro de la Ley 1273 de 2009 en su artículo 269B de la siguiente manera:

"El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones ".

Interceptación de datos informáticos.

Este tipo de delito se comisiona cuando el delincuente intenta o accede a una parte de un sistema o por ejemplo a una base de datos sin autorización alguna, con el fin de sacar copia de ficheros, información confidencial, entre otras, esta conducta delictiva es difícil de detectar por los

profesionales idóneos en la materia, puesto que este tipo de delito no deja huellas, salvo que el delincuente cometa un error que permita establecer la intrusión como tal.

Este delito es enunciado dentro del marco legal colombiano en la Ley 1273 de 2009 en su artículo 269 Como:

—[…] El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte […].

Daño Informático. Cuando se habla de daño a la información se debe tener en cuenta toda acción que afecte o vulnere la integridad de la información mediante el borrado, el deterioro, destrucción o alteración para cometer un ilícito que deje algún tipo de beneficio económico o de cualquier otra índole. Esta conducta delictiva es una de las comunes y no sólo se refiere a la información como archivos o el daño a aplicaciones, sino que también debe hacer referencia al daño que se pretenda materializar en contra de cualquier elemento lógico o físico que haga parte de un sistema.

La ley colombiana en el artículo 269D contenido en la Ley 1273 de 2009, lo contempla de la siguiente manera:

—[…] El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos […]

Uso de software malicioso. Este delito hace referencia al sabotaje informático mediante el uso de software tipo gusano, malware o troyano que la persona de forma ilícita infiltre en un sistema sin que el administrador del mismo note su presencia. Este tipo de ataque pretende dañar la información mediante su borrado o también se puede denegar algún servicio del sistema como

por ejemplo el bloqueo del antivirus o cualquier otra aplicación que no permita el correcto funcionamiento del mismo, impidiendo la realización de alguna actividad fomentando demoras en los procesos.

La Ley 1273 de 2009 describe este delito dentro del artículo 269E de la siguiente manera:

―[…] El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos […]

Violación de da tos personale. Toda aquella persona que mediante alguna herramienta busque divulgar o vender información que es confidencial a través de medios telemáticos o físicos y que pueda causar daños materiales, personales o económicos esta incurriendo en violación a los datos personales, esta situación es utilizada en muchas ocasiones con el fin de lucrarse de una forma ilícita sin respetar la propiedad intelectual o la intimidad de las personas, un ejemplo de este tipo de delito son las imágenes explicitas o videos íntimos publicados en diferentes medios como redes sociales.

Según el Abogado Martí Manent este delito se define como ―En el ámbito de la regulación del tratamiento de datos personales, la violación de datos personales es toda violación de la seguridad que ocasione la destrucción accidental o ilícita, la pérdida, alteración, comunicación no autorizada de datos personales transmitidos, conservados o tratados de otra forma, o el acceso a estos.

En este ámbito la legislación colombiana se ampara en la Ley estatutaria 1581 de 2012 reglamentada por el decreto nacional 1377 de 2013, mediante la cual se dictan disposiciones para la protección de datos personales y define el dato personal dentro de su artículo 3 numeral C,

como ―Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables

De acuerdo a la Ley 1273 de 2009 este delito se contempla en el artículo 269F, el cual lo cita de la siguiente manera:

―[…] El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes […]

Suplantación de sitios web para capturar datos personales. Este delito hace referencia al famoso Phishing y hace parte de los ataques de ingeniería social, los cuales se han perpetuado valiéndose de las vulnerabilidades no de los sistemas informáticos sino de los errores o fallos humanos, mediante los cuales logran conseguir datos personales que puedan servir para engañar y sustraer información. Este tipo de actividades delictivas utilizan varias formas de operar como por ejemplo llamadas telefónicas, envió de correos electrónicos en donde solicitan información sensible como claves de tarjetas de crédito o inclusive en forma física con identificaciones falsas para lograr el acceso a sitios no autorizados al público en las entidades.

La ley colombiana en el artículo 269G de la Ley 1273 de 2009 lo enuncia como:

―[…] El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes […]

Hurto por medios informáticos y semejantes . Se considera hurto a toda aquella acción ilícita en donde se busque apoderarse de un bien ya sea inmueble o en este caso llevado a la informática, un archivo físico o digital conservado en una entidad. Este delito puede comisionarse por medio de herramientas o técnicas que no requieran de violencia o la

intimidación de personas, que a diferencia del robo, que es un hecho punible cometido mediante el uso de la fuerza y la intimidación para llegar a su feliz término.

En el caso de la ciberdelincuencia, este hecho se puede materializar mediante el uso de correos electrónicos falsos, violación de la seguridad de un sistema o algún tipo de ingeniería social, el artículo 239 del código penal colombiano, en su titulo

VII de la Ley 599 de 2000 define el hurto como ―El que se apodere de una cosa mueble ajena, con el propósito de obtener provecho para sí o para otro

Por su parte, en la ley 1273 de 2009 se amplia el concepto de hurto al ámbito informático contemplado en el artículo 269I de la siguiente manera:

―[…] El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos

El cual hace énfasis en lo estipulado en el código penal y cuyas penas también se rigen por el mismo en el Artículo 240.

En Colombia dentro del ámbito del derecho público de los derechos fundamentales del acceso a la información, el buen nombre y la intimidad están reglamentados en el artículo 15 de la Constitución política colombiana de 1991, el cual cita lo siguiente:

―Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución. La

correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptados o registrados mediante orden judicial, en los casos y con las formalidades que establezca la ley

A este artículo se le une, la Ley 57 de 1985 en su Capitulo II denominado ―Acceso ciudadano a los documentos, donde cada artículo que compone este capitulo de la Ley hace énfasis en el derecho que tienen los ciudadanos para consultar su información personal y el acceso a documentos públicos que se encuentren disponibles.

Otras leyes que regulan estos derechos en Colombia son:

El Código Contencioso-Administrativo (Dec.01/84, Dec.2304/89 y ley 446 de 1998) en su Capitulo IV ―Del derecho de petición de informaciones‖

La Ley 44 de 1993 del 5 de febrero de 1993, por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944. La cual hace énfasis sobre los derechos de autor

La Ley 527 de 1999 del 18 de agosto, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

La Ley 599 y 600 de 2000, Códigos Penal y Procesal Penal Colombiano

Ley 1266 de 2008 de diciembre 31, por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones

Ley estatutaria 1581 de 2012 Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones generales para la protección de datos personales.

Y más recientemente la ley 1273 de 2009 de Enero 5, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Evolución de la legislación en Venezuela.

Este país hacia el año 1999 acogió el ―habeas data‖ dentro de su constitución política, así mismo consagró o estipuló la inviolabilidad de las comunicaciones privadas, el derecho a la protección del honor, vida privada, intimidad, imagen, confidencialidad y reputación, esto fijando limitaciones o parámetros que permitieran un control sobre la informática y las nuevas tecnologías frente a la intimidad de sus ciudadanos.

Dentro de esta ley se denotan los delitos informáticos como:

Acceso indebido. ―Toda persona que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema que utilice tecnologías de información

Sabotaje o daño a sistemas. ―Todo aquel que con intención destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualesquiera de los componentes que lo conforman

Favorecimiento culposo del sabotaje o daño. ―Si el delito previsto en el artículo anterior se cometiere por imprudencia, negligencia, impericia o inobservancia de las normas establecidas, se aplicará la pena correspondiente según el caso, con una reducción entre la mitad y dos tercios

Posesión de equipos o prestación de servicios de sabotaje. ―Quien importe, fabrique, distribuya, venda o utilice equipos, dispositivos o programas, con el propósito de destinarlos a

vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información; o el que ofrezca o preste servicios destinados a cumplir los mismos fines

Espionaje informático. —Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes […]

Falsificación de documentos. —Quien, a través de cualquier medio, cree, modifique o elimine un documento que se encuentre incorporado a un sistema que utilice tecnologías de información; o cree, modifique o elimine datos del mismo; o incorpore a dicho sistema un documento inexistente […]

Hurto. —Quien a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema o medio de comunicación para apoderarse de bienes o valores tangibles o intangibles de carácter patrimonial sustrayéndolos a su tenedor, con el fin de procurarse un provecho económico para sí o para otro […]

Fraude.—Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos contenida, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un provecho injusto en perjuicio ajeno […]

Manejo fraudulento y apropiación de tarjetas inteligentes o instrumentos análogos. —Toda persona que por cualquier medio cree, capture, grabe, copie, altere, duplique o elimine la data o información contenidas en una tarjeta inteligente o en cualquier instrumento destinado a los mismos fines; o la persona que, mediante cualquier uso indebido de tecnologías de información, cree, capture, duplique o altere la data o información en un sistema, con el objeto de incorporar usuarios, cuentas, registros o consumos inexistentes o modifique la cuantía

de éstos […] y por otro lado en el artículo 17 hace referencia a la apropiación como ―Quien se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se haya perdido, extraviado o que haya sido entregado por equivocación, con el fin de retenerlo, usarlo, venderlo o transferirlo a una persona distinta del usuario autorizado o entidad emisora […]

Violación a la privacidad. ley especial contra delitos informáticos en el Capítulo III, en el cual en cada uno de los artículos que lo componen se consagra los diferentes aspectos sobre esta problemática.

Pornografía infantil. Este delito realmente es nuevo por lo que hasta mediados del siglo XX, se le comienza a dar un tratamiento dentro de los diferentes códigos penales y ahora con el auge de la informática y las telecomunicaciones, se le da un tratamiento más acorde pensando en la protección de los niños, niñas y adolescentes en mantener su integridad física y moral incorrupta y en ofrecerles un mejor futuro libre de amenazas y riesgos que atenten contra su integridad como personas. En este caso no es la excepción la legislación venezolana que ha involucrado esta temática dentro de su ley especial y que por ende busca sancionar de manera severa a quien atente contra los niños, niñas y adolescentes publicando, transmitiendo o se valga de algún medio informático para llevar a cabo esta actividad delictiva, es así como en el Capítulo IV se consagra este hecho punitivo.

Propiedad intelectual y oferta engañosa. Por esta razón, se incluye un capitulo en donde se consagra propiamente la violación a la propiedad intelectual y la oferta engañosa en el Capítulo V en donde se definen jurídicamente y se sancionan estos delitos.

Evolución de la legislación Argentina frente a los delitos informáticos. En Argentina hace algunos años no era considerada la información como algo tangible, por lo tanto solo

estaban protegidos los lenguajes de bases de datos y algunas plantillas de cálculo y lo que estos a su vez contuvieran.

Protección de datos personales y privacidad. La ley mediante la cual se ampara estos dos aspectos en Argentina es la Ley 25.326, sancionada el 4 de octubre de 2000 y promulgada el 30 de octubre de ese mismo año, en la cual se dictan las disposiciones generales y especificas por las cuales se protege la privacidad. Propiedad intelectual. Este tema esta amparado mediante la ley 11.723 denominada ―Régimen legal de la propiedad intelectual‖, mediante la cual se protege la propiedad intelectual y se dictan disposiciones legales generales y especificas concernientes a este ámbito, como el registro de las obras, la venta, derechos y disposiciones especiales. También se dictan sanciones penales y económicas a quienes incurran en los delitos que permitan su violación.

Promoción de la industria del software. Se crean la Ley 25.856 denominada Consideración de la producción de software como actividad industrial, en la cual se dictan las disposiciones generales que abarcan este tema en sus cuatro artículos y la Ley 25.922 denominada Ley de promoción de la industria del software‖, compuesta por seis capítulos en los cuales se consagra las disposiciones generales, infracciones y sanciones respecto a la promoción o comercialización del software y su producción como actividad industrial.

Delitos informáticos y ciberseguridad. La Ley que permite brindar protección en contra de los abusos en el acceso de la información, fraude, hurto y demás delitos informáticos en Argentina se denomina Ley 26.388 sancionada en Junio de 2008 y por medio de la cual se modifica el código penal argentino, incluyendo de esta manera todos los aspectos concernientes a la violación de secretos.

Evolución de la legislación Chilena frente a los delitos informáticos.

Chile fue el primer país de Latinoamérica en crear un bien jurídico para el uso de la informática, fue una adición al código penal chileno con el fin de proteger los nuevos bienes que surgen con el auge de la tecnología y que mediante la creación de figuras penales especiales, busca evitar las interpretaciones extensivas de las normas penales tradicionales, incluyendo de esta manera las conductas indebidas contra los sistemas de información tanto para el soporte lógico como para los datos que se manejan.

De la misma manera, Chile mediante sus herramientas jurídicas hace referencia a la protección de propiedad intelectual y protección de datos.

Propiedad intelectual. En este aspecto Chile promulgo la ley 17.336 del 2 de octubre de 197040, la cual protege los derechos de autor, la moral y establece sanciones y disposiciones legales para cubrir las necesidades jurídicas frente a este tema.

Protección de datos. Se promulga la Ley 19.628 denominada ―Protección de datos de carácter personal promulgada el 28 de agosto de 1999, por la cual se dictan disposiciones legales para proteger el manejo de datos personales en todos los ámbitos.

Delitos informáticos . El 7 de junio de 1993 fue publicada la Ley 19.223 denominada ―Ley relativa a delitos informáticos, en donde se tipifican figuras penales relativas al uso de la informática. Este bien jurídico se basa en la protección de la propiedad intelectual y se constituye de cuatro artículos los cuales consagran los delitos más comunes como el espionaje, sabotaje, daño, entre otros.

Documento electrónico. Se crea la Ley 19.799 denominada ― Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma, por la cual se dictan

todas las disposiciones pertinentes que sancionen las infracciones contra estos bienes y servicios, aparte de amparar a los usuarios y la información contenida en los mismos.

Seguridad Informática. Existen varias definiciones acerca de lo que realmente abarca la seguridad informática y su importancia dentro del desarrollo tecnológico actual, de todas estas definiciones la más completa es la proporcionada por ISO/IEC 27001 y que fue aprobada y publicada en el año 2005 por la International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC):

"La seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

En ese orden de ideas es bueno enunciar lo que dice Jorge Sendra Mas, quien indica lo siguiente: La Seguridad de la Información ha experimentado una continua evolución durante la última década, desde un enfoque puramente tecnológico, donde las necesidades se cubren mediante la adquisición de herramientas con el fin de mitigar las últimas vulnerabilidades conocidas, hasta un enfoque dominado por la necesidad de justificar las inversiones en seguridad de la información, como un activo esencial. Este enfoque se basa en una gestión continua de los riesgos sustentados en la optimización de ratios empresariales como es el de coste/beneficio.

Marco Contextual

El presente proyecto de investigación basamos la aplicación de los delitos informáticos en Colombia en donde se promulgo la ley 1273 el 5 de enero de 2009, antes de dicha ley en

Colombia se había implementado el Decreto 1360 de 1986 con el cual se reglamentaba la inscripción de software o soporte lógico en el Registro Nacional de Derecho de Autor, el cual ayudo a proteger los derechos de autor sobre los software que las personas crearan.

A si mismo se establecen los decretos reglamentarios para la protección de los derechos de autor como lo establecen los artículos 51 y 52 del Capítulo IV de la Ley 44 de 1993, con esto se crean las primeras normas que logran sancionar las personas que violan estos derechos y se convierten en base para la reforma al código penal colombiano del año 2000: Capítulo Único del Título VII que determina los Delitos contra los Derechos de Autor: Artículo 270: Violación a los derechos morales de autor. Artículo 271: Defraudación a los derechos patrimoniales de autor. Artículo 272: Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones.

Por su parte, el código penal colombiano (Ley 599 de 2000) estipula en el libro II Capítulo VII del Título III: Delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones:

Artículo 192

Violación ilícita de comunicaciones. Artículo 193: Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Artículo 194: Divulgación y empleo de documentos reservados. Artículo 195: Acceso abusivo a un sistema informático. Artículo 196: Violación ilícita de comunicaciones o correspondencia de carácter oficial.

Artículo 197.

Utilización ilícita de equipos transmisores o receptores. Estos artículos son concordantes con el artículo 357: Daño en obras o elementos de los servicios de comunicaciones, energía y combustibles.

Otra norma posterior a esta, fue la Ley 679 de 2001, la cual consagró un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores. Por otra parte, genera restricciones a los proveedores o servidores de internet, en donde se encuentren archivos, imágenes, textos o documentos relacionados con contenido sexual con menores de edad.

Sin embargo, esta Ley no toma como delitos informáticos estas actitudes delictivas, por lo que sólo son sanciones de tipo administrativo, de acuerdo a lo consagrado en el Artículo 10 del mismo. Por lo que el 21 de julio del año 2009 se sanciona la Ley 1336 "por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual, con niños, niñas y adolescentes", de esta forma tratar de subsanar las falencias de la anterior Ley 679 de 2001 y a través de esta imponer sanciones de tipo penal a las conductas delictivas en favor de los menores y en contra de la pornografía infantil.

En el mismo sentido, se puede decir que a través del tiempo Colombia ha sido afectada por los delitos cometidos mediante el uso de los avances tecnológicos, los cuales se pueden dividir a nivel general en:

Fraudes: en este punto se hace referencia a los delitos como los datos falsos o engañosos, manipulación de datos de entrada y salida, manipulación de programas, falsificaciones informáticas y phishing.

Robo de servicios: son delitos cuyo objetivo es causar daños patrimoniales mediante técnicas poco usuales y que llegan a pasar desapercibidas como el hurto de tiempo del computador o

internet, la apropiación de información residual o basura (Scavenging), el parasitismo informático y la suplantación.

Delitos de espionaje y hurto informático: en este caso aparecen los casos de fuga de datos o que es lo mismo la divulgación sin autorización de información y la reproducción no legítima de programas informáticos o cualquier otra obra de forma fraudulenta.

Sabotaje informático: tienen que ver con la modificación o borrado de datos y la obstaculización de funciones dentro de un sistema informático, en este caso se tienen los gusanos, las bombas lógicas, virus, malware, ciberterrorismo y los ataques DDoS o de denegación de servicio.

Delitos de acceso no autorizado a servicios informáticos: tal vez de los más comunes y más populares, cuyo fin es el mismo que todos los anteriores delitos descritos, acceder a información para lucrarse de la misma o causar daños. Dentro de este tipo de delitos están las puertas falsas, la llave maestra, el pinchado de líneas y los que cometen los piratas informáticos (Hackers).

Aparte de este tipo de delitos, en Colombia se presentan una nueva modalidad de delitos que hasta ahora se están conociendo, los cuales se cometen a través del uso de redes sociales (Facebook, Twitter, Instagram, Youtube, etc.) y aún se están tratando de clasificar para realizar un tratamiento penal contra los mismos y contra las personas que los cometen, dentro de estos se encuentran:

Ciber Bulliying: este delito se ha venido presentando con fuerza en Colombia a través de las redes sociales y consiste en la intimidación y agresión utilizando estos medios entrando en un tipo de atentado contra la moral y la integridad de la persona.

Perfiles falsos: este delito es un tipo de suplantación de identidad, pero en este caso la finalidad es atentar contra la dignidad e integridad moral y psicológica de las personas mediante

la creación de un perfil falso y realizando publicaciones que atenten contra la victima. Este delito se esta volviendo cada día más común en Colombia por el uso excesivo de redes sociales y el suministro de información de tipo personal en las mismas.

Pornografía infantil: este delito tiene alta incidencia, puesto que en las redes sociales abundan los pedófilos en busca de menores que inocentemente son seducidos al ser contactados por el criminal, el cual busca ganarse su confianza para luego obtener videos y fotografías de tipo sexual de los menores, material que después es difundido por internet.

Sexting: se trata de compartir contenidos íntimos a través de mensajería móvil como por ejemplo whatsapp o chat de cualquier otra red social, en donde en primera medida se busca un encuentro sexual sin transcendencia que luego puede llegar a algo mas explicito de acuerdo a la situación. Este tipo de actuaciones ponen en riesgo la intimidad del emisor del mensaje, debido a que el contenido queda expuesto a graves riesgos como la publicación de este tipo de contenidos en redes sociales como parte de venganzas de parejas cuya relación ya terminó o pueden ser utilizadas para el chantaje a cambio de no ser divulgadas.

Marco Legal

En Colombia los delitos informáticos se sancionarán mediante la ley 1273 de Enero 5 de 2009 por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Dentro de esta ley se estipulan 10 delitos informáticos agrupados en dos capítulos que los sancionan de la siguiente manera:

Capitulo I - De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269A: Acceso abusivo a un sistema informático

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.

Artículo 269C: Interceptación de datos informáticos.

Artículo 269D: Daño Informático.

Artículo 269E: Uso de software malicioso.

Artículo 269F: Violación de datos personales.

Artículo 269G: Suplantación de sitios web para capturar datos personales.

Artículo 269H: Circunstancias de agravación punitiva

Capitulo II - De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes

Artículo 269J: Transferencia no consentida de activos.

Ley estatutaria 1581 de 2012: por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1266 de 2008: por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

La Ley 527 de 1999 del 18 de agosto, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

La presente ley será aplicable a todo tipo de información en forma de mensaje de datos, salvo en los siguientes casos:

a) En las obligaciones contraídas por el Estado colombiano en virtud de convenios o tratados internacionales;

b) En las advertencias escritas que por disposición legal deban ir necesariamente impresas en cierto tipo de productos en razón al riesgo que implica su comercialización, uso o consumo

- Ley 23 de 1982. Sobre los derechos de autor: presenta todas las disposiciones generales y especiales que regulan la protección del derecho de autor en Colombia. el artículo 21 de la Ley 23 de 1982 establece el plazo de protección de los derechos de autor, aplicable: la vida del autor y ochenta años después de su muerte.
- La Ley 44 de 1993: por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.

En argentina se estipuló la ley especial contra los delitos informáticos que modificó el código penal de dicho país en aras de proteger los datos y la información a nivel nacional, esta ley 26.388 sancionada el 4 de Junio de 2008 y promulgada en hecho el 24 de Junio del mismo año tipifica y penaliza los siguientes delitos informáticos:

- Pornografía infantil por Internet u otros medios electrónicos (art. 128 CP);
- Violación, apoderamiento y desvío de comunicación electrónica (art. 153, párrafo 1º CP);
- Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (art. 153, párrafo 2º CP);
- Acceso a un sistema o dato informático (artículo 153 bis CP);
- Publicación de una comunicación electrónica (artículo 155 CP);

- Acceso a un banco de datos personales (artículo 157 bis, párrafo 1º CP);
- Revelación de información registrada en un banco de datos personales

|(artículo 157 bis, párrafo 2º CP);

- Inserción de datos falsos en un archivo de datos personales (artículo 157 bis, párrafo 2º CP; anteriormente regulado en el artículo 117 bis, párrafo 1º, incorporado por la Ley de Hábeas Data);
- Fraude informático (artículo 173, inciso 16 CP);
- Daño o sabotaje informático (artículos 183 y 184, incisos 5º y 6º CP).

Por otro lado, Chile fue el primer país latinoamericano en penalizar los delitos informáticos y tipificarlos dentro de su legislación denominando a esta ley 19223 Ley Relativa a los delitos informáticos y que sanciona los delitos informáticos de la siguiente manera:

Artículo 1. El que maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida, obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor en su grado medio a máximo.

Artículo 2. El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.

Artículo 3. El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.

Artículo 4. El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.

Y por último se observa una de las leyes que hacen parte del comparativo que se realizará en el marco del desarrollo del presente proyecto, la cual también aporta de manera significativa en la penalización y tipificación en la comisión de delitos informáticos a nivel latinoamericano, esta norma es denominada ―Ley especial contra los delitos informáticos‖ que fue sancionada y publicada para su vigencia en Venezuela el 30 de octubre de 2001 en la gaceta oficial de la república bolivariana de Venezuela, siendo esta una de las leyes más recientes en penalizar este tipo de delincuencia y lo realiza de la siguiente forma:

Título II – De los delitos.

Capítulo I - De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información.

- Artículo 6. Acceso indebido
- Artículo 7. Sabotaje o daño a sistemas
- Artículo 8. Favorecimiento culposo del sabotaje o daño
- Artículo 9. Acceso indebido o sabotaje a sistemas protegidos
- Artículo 10. Posesión de equipos o prestación de servicios de sabotaje.
- Artículo 11. Espionaje informático.
- Artículo 12. Falsificación de documentos

Capítulo II - De los Delitos Contra la Propiedad

- Artículo 13. Hurto.
- Artículo 14. Fraude.
- Artículo 15. Obtención indebida de bienes o servicios.
- Artículo 16. Manejo fraudulento de tarjetas inteligentes o instrumentos análogos.
- Artículo 17. Apropiación de tarjetas inteligentes o instrumentos análogos.
- Artículo 18. Provisión indebida de bienes o servicios.

- Artículo 19. Posesión de equipo para falsificaciones.

Capítulo III - De los Delitos Contra la Privacidad de las Personas y de las Comunicaciones

- Artículo 20. Violación de la privacidad de la data o información de carácter personal
- Artículo 21. Violación de la privacidad de las comunicaciones
- Artículo 22. Revelación indebida de data o información de carácter personal

Capítulo IV - De los Delitos Contra Niños, Niñas o Adolescentes

- Artículo 23. Difusión o exhibición de material pornográfico.
- Artículo 24. Exhibición pornográfica de niños o adolescentes.
- Capítulo V - De los Delitos Contra el Orden Económico
- Artículo 25. Apropiación de propiedad intelectual.
- Artículo 26. Oferta engañosa.

Metodología

Paradigma de la Investigación.

Esta investigación se planteó desde el método de investigación científica cualitativa, así en la cual se desarrolló el tema concretando diferentes estrategias que desde el estudio de documentos implicaron la utilización y el análisis de una variedad de materiales tales como la ley 1273/2009, jurisprudencia, artículos de investigación respecto del tema de hurto por medios informáticos y semejantes y los delitos informáticos, los cuales abordan el tema de manera directa desarrollando esta problemática social-jurídica.

Enfoque de la Investigación.

El tipo de estudio realizado obedece a un sistema exploratorio descriptivo, en el que el problema de investigación es un tema poco abordado y descriptivo porque muestra desde la perspectiva del Derecho la realidad del tipo penal HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES ARTÍCULO 269I: (Ley 1273 de 2009) desde el análisis propio a la legislación en Colombia sobre este delito.

Población y Muestra.

Este trabajo de Investigación de Derecho, por ser de carácter descriptivo, documental, cualitativo, académico, doctrinario, literario, y jurisprudencial, no requiere toma de población ni de muestra, puesto que se centra en un tipo penal específico.

Diseño de la Investigación

El diseño metodológico empleado en este proyecto de investigación jurídica se realizó de acuerdo a un estudio descriptivo-analítico de índole jurídico, en el que se han debatido a través de las normas existentes en Colombia con el tutor metodológico y otros docentes con el conocimiento del tema de estudio acerca de algunas de las maneras en que se puede realizar análisis socio-jurídico del tema teniendo en cuenta que se trata de un problema de investigación relacionado con un tipo penal y que a su vez debido a su rápida evolución ha afectado el conjunto social; a partir de lo anterior se darán a conocer unas conclusiones sobre el tema de estudio y posibles soluciones sobre este asunto y problema de investigación que se desarrolla en este proyecto.

Técnicas e Instrumentos de Recolección de Datos

Las técnicas empleadas para desarrollar la investigación, así como las fuentes de información para la elaboración de la misma fueron:

Análisis y revisión documental, la Ley, la Jurisprudencia de la Corte Suprema de Justicia y de la Corte Constitucional, artículos de investigación respecto del tema de delitos informáticos, esto con el fin de dar a conocer la problemática social-jurídica que implica el tipo penal que es objeto de estudio revelando el fenómeno presente y actual del mismo y a su vez evolución del mismo frente a la legislación en Colombia.

Análisis de los resultados

Resultados

Modalidades de hurtos por medios informáticos y semejantes en transacciones bancarias en personas naturales que se han generado en el Municipio de San José de Cúcuta en el período 2016-2017.

Las innovaciones tecnológicas se están desarrollando de forma constante en la sociedad, siendo utilizada para la obtención de beneficios en diferentes escenarios, especialmente en el relacionado con el de la comunicación. Cada integrante de la sociedad participa de forma activa en la utilización de estos medios, argumentando que son realmente importantes y trascendentales para la actualidad.

Las instituciones bancarias se han encargado de establecer entre sus diferentes procedimientos el uso de las herramientas tecnológicas, ofreciendo la facilidad en el desarrollo de ellas, sin embargo, ante esto, se han presentado diferentes problemáticas, especialmente la comisión de conductas punibles enfatizadas en el hurto ha sido uno de los factores más importantes y preocupantes que se presenta en la sociedad actual y especialmente porque no existe una protección adecuada por parte de las autoridades.

Este tipo de acciones no desarrolla ningún tipo de delimitación hacia la sociedad, es decir, sus actuaciones son ejecutadas sin tener presente el estrato social de las víctimas, lo único que identifican es el ámbito económico.

El desarrollo de Internet y de las nuevas tecnologías asociadas a la red relacionadas con la información y las comunicaciones hace del ciberespacio un nuevo lugar para la perpetración de

distintos ataques a bienes jurídicos tan importantes como la intimidad, el honor, la propiedad, la libertad sexual y hasta la integridad física y la vida. Aunque la mayoría de las conductas no son, en esencia, algo nuevo en sí mismas la extraordinaria particularidad del medio con el que se cometen, o sobre el que actúan, confiere a estas conductas una especial configuración que obliga a romper los esquemas clásicos para su investigación y enjuiciamiento.

Afortunadamente el Derecho Penal y el Derecho Procesal Penal han evolucionado para enfrentarse a ese nuevo cauce de ejecución delictiva que se desarrolla en un ámbito virtual y tecnológico, diferente al modelo tradicional de criminalidad física, individual e interpersonal, ya que cuestiona los axiomas vigentes.

Precisamente por esto consideramos de interés realizar en este artículo una especial referencia, desde el punto de vista procesal, a las más importantes particularidades que ofrece la investigación y enjuiciamiento de estas conductas delictivas comprendidas bajo el término cibercrimen.

El ordenamiento jurídico en Colombia ha establecido diferentes actuaciones para proteger a la sociedad ante este tipo de problemáticas, sin embargo, esta situación no solamente se relaciona con la protección que debe ofrecer el órgano coercitivo sino con la incredulidad existente en la sociedad en el desarrollo de estos procedimientos en donde se puede analizar que esta es la causa que más incide para que se cometan los delitos.

La ciudad de Cúcuta no se encuentra exenta de esta problemática e infortunadamente ha sido una de las más afectadas por esta situación, en donde las autoridades de diferentes maneras han establecido las actuaciones pertinentes para la protección de las personas en su ámbito económico.

Una de las problemáticas más preocupantes consiste en que la sociedad colombiana implementa diferentes estrategias para realizar los hurtos por medio de las innovaciones tecnológicas, lo que conlleva a determinar el problema cultural que posee la sociedad en vulnerar los bienes jurídicos que han sido tutelados por medio del ordenamiento jurídico colombiano, entre ellos el del patrimonio cuando se cometen los hurtos.

La manipulación es una de las actuaciones ejecutadas constantemente, en este escenario es pertinente identificar los tipos de procedimientos que se llevan cabo:

Manipulación de los datos de entrada:

Este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

Las entidades bancarias han establecido estrategias de protección ante este tipo de situaciones, sin embargo, las persona del común no tiene en cuenta todos los aspectos que se han mencionado para su protección, lo que genera una mayor facilidad por parte de los delincuentes en cometer este tipo de conductas.

Manipulación de programas:

Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya, que consiste en insertar

instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

Esta metodología está siendo utilizada comúnmente por la sociedad en general, y en ella se pretende que la persona reciba un mensaje o algún tipo de información para que la herramienta tecnológica sea invadida y se obtenga información importante sobre ella, obteniendo entre ellas claves, usuarios y acceso a diferentes cuentas, principalmente las informáticas.

Manipulación de los datos de salida:

Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían a base de tarjetas bancarias robadas; sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

Otro de los escenarios que se identifica es la modificación de los cajeros automáticos en donde las personas ingresan sus claves con la mayor confianza del mundo sin tener presente que estos medios están siendo alterados para obtener información pertinente, que permita más adelante extraer dinero de forma fácil.

Manipulación informática aprovechando repeticiones automáticas de los procesos de cómputo:

Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra (Hall, s.f.).

Procedimiento penal realizado al delito de hurto por medios informáticos en el Distrito Judicial de Cúcuta en los años 2016-2017.

En los delitos en que la acción y el resultado se producen dentro de un mismo Estado resulta aplicable la ley de ese Estado, cualquiera que sea la nacionalidad del autor. Aún en estos casos la complejidad es considerable pues para determinar el juzgado competente no está claro cuál es el criterio aplicable: el domicilio del querellado, el lugar en el que se ejecutó el delito, el de ubicación del servidor, aquel en el que se descubrieron las pruebas materiales, el lugar en que se iniciaron las actuaciones procesales, el lugar en el que se produjeron los daños, etc. En estos casos habrá que referirse en principio al lugar en que se perpetró la acción.

Mayores problemas surgen con los delitos perpetrados a distancia, muy frecuentes en Internet, y en los que la acción y el resultado se producen en diferentes países8. La doctrina y la jurisprudencia se han manifestado más favorables a apreciar la teoría de la ubicuidad que tiene en cuenta como lugar de comisión del delito tanto el lugar en el que se ha producido la acción como el resultado dañoso.

El Estado colombiano en su ordenamiento jurídico identifica de forma clara la situación que se está presentando en la sociedad, especialmente en lo relacionado con los delitos informáticos siendo pertinente la promulgación de preceptos jurídicos y legales para proteger a la sociedad sobre estas actuaciones.

El procedimiento penal realizado sigue siendo el mismo y se identifica en el ordenamiento jurídico colombiano, especialmente en el Código Penal y en el Código de Procedimiento Penal, sin embargo, es necesario hacer énfasis del precepto legal que se establece en relación a estas situaciones problemáticas y vulneradoras de los derechos de las personas.

La Ley 1273 del 2009 por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Esta normativa se caracteriza por ser el medio jurídico de gran importancia ante la protección de la información y de los datos, siendo el bien jurídico tutelado por parte de los preceptos legales, con el ánimo de conocer a mayor profundidad los aspectos que se han establecido en relación a las conductas punibles desarrolladas sobre este ámbito.

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

En este escenario el aparato legislativo pretende proteger las actuaciones abusivas que son desarrolladas por parte de las personas cuando exista una autorización o no, sin embargo, establece que frente a la primera circunstancia se ha desarrollado una extralimitación de las funciones que han sido consignadas. Se puede añadir que existe un exceso de confianza lo cual motiva a que se ejecute la comisión de la conducta punible.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y

ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

La facultad es uno de los aspectos más importantes en esta tipificación, argumentando que el que no este será sancionado por realizar impedimentos para la obtención de información, circunstancia que se presenta constantemente bloqueando los portales informáticos y demás servidores.

Artículo 269C: Interceptación de datos informáticos.

"El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses."

Otra de las situaciones que se presente en relación a los delitos informáticos corresponde a la interceptación, consistiendo principalmente en obtener datos de forma ilegal sin alguna autorización judicial. Este escenario se ha desarrollado en diferentes oportunidades en el país, generando controversia, especialmente porque la realización de estas actuaciones es implementada por altos funcionarios del gobierno, en síntesis, de dirigentes políticos.

Artículo 269D: Daño Informático.

"El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes."

La eliminación de la información es otro de los escenarios que se tiene en cuenta frente a los daños informáticos que se presenta, este tipo de acciones se relaciona con la perdida de información y ha sido evidenciado principalmente en ataques que se ejecutan hacia las plataformas del Estado colombiano.

Artículo 269E: Uso de software malicioso.

"El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes."

Este tipo de delito se relaciona con lo expuesto sobre las formas en cómo se vulneran los derechos y es una de las estrategias para extraer información trascendental, especialmente sobre cuentas bancarias obteniendo acceso a ella.

Artículo 269F: Violación de datos personales.

"El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes (Congreso de Colombia, 2009)."

Finalizando lo relacionado con la protección jurídica que establecen las normas en el país, se argumenta que es uno de los escenarios más importantes para la seguridad ciudadana, lo cual ha generado que la sociedad tenga más confianza frente a las innovaciones tecnológicas que se están presentando constantemente y que son utilizadas para el desarrollo de transacciones bancarias.

Posibles soluciones con la finalidad de no ser víctima del delito de hurto a través de medios informáticos en el Municipio de San José de Cúcuta.

Ante las diferentes soluciones que se pueden implementar para que la persona no sea víctima de los delitos de hurto que son desarrollados por medios informáticos se pueden expresar diferentes conclusiones al respecto, las cuales serán descritas de forma ordenada para comprender que estrategias son adecuadas ante esta situación.

En primer lugar se debe mencionar que la comisión de conductas punibles son acciones que se ejecutan desde diferentes directrices, entre ellas las endógenas y exógenas que inciden para que la persona cometa la acción. El Estado colombiano, en su artículo segundo, señalada una serie de finalidades para la sociedad, sin embargo, la posibilidad de ser ejecutadas se caracterizan por ser utópicas ante los obstáculos y demás dificultades que son evidenciadas.

Las soluciones se enmarcan en dos escenarios, el primero consiste en la eliminación de la conducta punible y seguidamente se puede mencionar las alternativas a ejecutar por parte de la sociedad en general para el desarrollo de su propia protección, entre ellas están:

Utilice contraseñas seguras, es decir, aquellas compuestas por ocho caracteres, como mínimo, y que combinen letras, números y símbolos. Es conveniente además, que modifique sus contraseñas con frecuencia. En especial, le recomendamos que cambie la clave de su cuenta de correo si accede con frecuencia desde equipos públicos.

Navegue por páginas web seguras y de confianza. Para diferenciarlas identifique si dichas páginas tienen algún sello o certificado que garanticen su calidad y fiabilidad. Extreme la precaución si va a realizar compras online o va a facilitar información confidencial a través de internet.

En la barra del navegador debe aparecer el icono del candado cerrado. A través de este icono se puede acceder a un certificado digital que confirma la autenticidad de la página. Sea

cuidadoso al utilizar programas de acceso remoto. A través de internet y mediante estos programas, es posible acceder a un ordenador, desde otro situado a kilómetros de distancia.

Presta especial atención en el tratamiento de su correo electrónico, ya que es una de las herramientas más utilizadas para llevar a cabo estafas, introducir virus, etc. (Recovery Labs, s.f.).

Todas estas indicaciones son dirigidas hacia las personas que utilizan estos medios tecnológicos, en donde se evidencian campañas de sensibilización para que la sociedad identifique plenamente los peligros que se pueden llegar a presentar a causa de esta problemática. Infortunadamente las personas no comprenden la realidad y no realizan ningún tipo de protección ante sus claves, específicamente las de las cuentas bancarias, lo cual conlleva a que se sigan presentando este tipo de procedimientos afectando a la sociedad en su patrimonio y en la información.

Las amenazas que se presentan con mayor constancia en el desarrollo de los delitos informáticos son:

Accesos no autorizados: El más común de los riesgos, la utilización de la cuenta de otro usuario para acceder a recursos no autorizados.

Fuga de información: En todo sitio existe información sensitiva que debe ser protegida. Ejemplo: password de cualquiera de nuestros servidores (equipo suministrador de información a la Red. Unidad central de procesamiento donde se almacena gran cantidad de programas y datos durante las 24 horas del día para después distribuirlas por medio de la red de computadoras a la que sirve).

La situación se facilitaría algo más si las entidades y organizaciones víctimas los denunciaran, pero sucede que no lo hacen por considerar que tales hechos pueden poner al descubierto las fallas de los sistemas, y en ocasiones la fiabilidad de los sistemas informáticos (Ecured, s.f.)

Discusión

Análisis documental del delito informático en Cúcuta hurto por medios informáticos y semejantes artículo 269i: (Ley 1273/2009)

El análisis documental desarrollado sobre el delito informático que se presenta en la ciudad de Cúcuta conlleva a determinar que es una de las problemáticas preocupantes y que cada día va aumentando considerablemente, especialmente, en relación a la mínima atención que es recibida por parte de los ciudadanos del común, específicamente, de aquellas personas que utilizan cuentas bancarias pero que no consideran en ningún momento las medidas pertinentes para desarrollar una protección adecuada.

La Policía Nacional cumple un rol importante en este escenario y frente a ello realiza actividades pedagógicas en las instituciones educativas en la ciudad de Cúcuta en donde exponen lo siguiente:

En el encuentro de seguridad informática, el cual se inició con los alumnos del colegio Manuel Antonio Rueda Jara, sede Antonio Nariño del Municipio de Villa del Rosario, los alumnos de los grados sexto, séptimo y octavo fueron instruidos en la forma en que deben dar uso de la internet, especialmente de las redes sociales como Twitter, Facebook e Instagram, activando los mecanismos de seguridad requeridos para evitar ser víctimas de hackers y pedófilos, entre otra amenazas.

Los uniformados explicaron inicialmente los delitos tipificados en el Código Penal, la forma como se presentan, las acciones judiciales que se ejecutan en caso de que se registren, las penas y multas económicas a las que se ven expuestos los responsables de su comisión (La Opinión, 2015).

Frente a estas actuaciones hay dos escenarios trascendentales, primero, por las actividades académicas implementadas en donde se puede sensibilizar a los más jóvenes (caracterizados por hacer uso de las herramientas tecnológicas con mayor constancia) en las problemáticas que se pueden llegar a presentar cuando no existe ningún tipo de protección debida hacia los datos y seguidamente por la función pedagógica para que comprendan los peligros latentes de forma constante en el uso de las redes.

La sociedad debe comprender que la mejor medida para solucionar estas problemáticas corresponde a la no exposición de las diferentes claves que se utilizan en relación a los sistemas bancarios, argumentando que cuando esta situación se presenta es muy difícil que el aparato judicial pueda cumplir sus funciones ante las infinidades de ataques cibernéticos que se presentan, esto se debe a que desde diferentes lugares se desarrollan las acciones delictivas en donde se necesita de una investigación amplia para identificar al victimario.

El Estado colombiano mediante sus preceptos legales desarrolla la protección adecuada, pero la realidad es otra y preocupa a la sociedad, principalmente porque no las políticas que se han implementado no llegan a solucionar esta problemática, circunstancia que se agrava ante la incredulidad por parte de la sociedad por las actuaciones que desarrollan las instituciones, justificando que son las principales entidades encargadas de cooperar en la comisión de conductas punibles vulnerando sistemáticamente los derechos de las personas.

Reflexiones Finales

Finalizando el desarrollo de la investigación se determina que los delitos informáticos se caracterizan por ser una de las nuevas tendencias utilizadas por la población criminal para la ejecución de la vulneración de los derechos de las personas, en donde el Estado colombiano, por medio del aparato legislativo ha determinado la protección aunque los resultados no sean los esperados.

Los preceptos legales son pertinentes para la sociedad porque por medio de ellos se identifica claramente la protección desarrollada por parte del Estado colombiano, sin embargo existe una clara división entre la realidad existente y lo determinado por parte de las normas jurídicas, específicamente en la incredulidad que se presenta desde la sociedad hacia las actuaciones que realiza el gobierno.

La persona que utilice las herramientas tecnológicas, especialmente en lo relacionado con las transacciones en la cuenta bancaria, deben ser conscientes de los riesgos que se pueden llegar a presentar, puesto que los ataques cibernéticos son ejecutados constantemente esperando que persona pueda ofrecer sus datos y demás información relacionada con las cuentas de los bancos.

La ciudad de Cúcuta ha sido una de las poblaciones utilizadas por parte de los criminales para desarrollar este tipo de procedimientos en donde identifican que la sociedad no interpreta el riesgo que esta presenta en el uso de las transacciones bancarias y en especial lo desarrollado mediante el uso de las herramientas tecnológicas.

Por último se añade que una de las actuaciones que utilizan las entidades bancarias corresponde a la sensibilización hacia sus usuarios para que no expongan su información ante los correos, llamadas y demás mensajes que son recibidos en donde se solicitan usuarios y claves, lo cual conlleva a que se puedan generar escenarios para la comisión de hurtos.

Recomendaciones

Entre las recomendaciones obtenidas en el cumplimiento de los objetivos planteados se puede añadir que el Estado cumple su función en un porcentaje incompleto para la protección de los derechos de las personas, en este caso de la información de datos y del patrimonio, no obstante, esta situación no es realmente satisfactoria porque las instituciones a causa de diferentes escenarios no pueden solucionar las problemáticas existentes en relación a la protección de los derechos de la sociedad en general.

La mejor estrategia que se puede implementar para eliminar esta situación consiste en que la sociedad pueda identificar las actuaciones que son adecuadas para que ningún extraño tenga acceso a la información que se suministra en los medios tecnológicos correspondientes a las entidades financieras y bancarias.

La investigación es un procedimiento adecuado para la identificación de causas y razones que inciden en las problemáticas sociales, en este caso, en el hurto por medio de delitos informáticos, frente a esta situación, es asertivo dar a conocer a la sociedad en general las estrategias que se pueden utilizar para que los victimarios no accedan a la información necesitada y se pueda proteger cualquier tipo de transacción. Esta situación realmente se basa es en el conocimiento de las actuaciones que conllevan a una mejor protección y no a la exposición de datos.

Referencias

Asamblea Nacional Constituyente. (1991). Constitución Política de Colombia de 1991. Bogotá: ANC.

Bolaños, A. y Narváez, T. (2014). Análisis comparativo sobre delitos informáticos en Colombia con relación a seis países de Latinoamérica. Tesis de grado, Pasto, Universidad Nacional abierta y a Distancia.

Congreso de Colombia. (2000). Ley 599. Por la cual se expide el Código Penal. Bogotá: El Congreso.

Congreso de Colombia. (2009). Ley 1273. Por la cual se modifica el Código Penal y se crea un nuevo bien jurídico denominado "de la protección de la información y de los datos". Bogotá: El Congreso.

Consejo de Europa. (2001). Convenio sobre la ciberdelincuencia. Budapest: Consejo de Europa.

Corte Suprema de Justicia Sala de Casación Penal. (2015). Sentencia SP1245 - 2015 M.P. Eyder Patiño Cabrera.

Días, M. (2006). Los delitos informáticos en Colombia y su penalización. Tesis de grado, Bogotá, Universidad Libre.

Ecured. (s.f.). Protección contra delitos informáticos. Recuperado de: https://www.ecured.cu/Proteccion_contra_delitos_informaticos

Granados, R. y Parra, A. (2015). El delito de hurto por medios informáticos que tipifican el artículo 269i de la ley 1273 del 2009 y su aplicación en el distrito judicial de Cúcuta en el periodo 2012 - 2014. Tesis de grado, San José de Cúcuta, Universidad Libre.

Hall, A. (s.f.). Tipos de delitos informáticos. Recuperado de: http://www.forodeseguridad.com/artic/discipl/disc_4016.htm

La Opinión. (2015). Enseñan en los colegios a eludir el delito informático. Recuperado de: https://www.laopinion.com.co/cucuta/ensenan-en-los-colegios-eludir-el-delito-informatico-101291#OP

Lima, M. (1984). Delitos electrónicos en criminalia. México: Academia Mexicana de Ciencias Penales.

Manjarrés, I. y Jiménez, F. (2012). Caracterización de los delitos informáticos en Colombia. Revista Pensamiento Americano, 5(9).

Miró, F. (2011). La oportunidad criminal en el ciberespacio, aplicación y desarrollo de la teoría de las actividades cotidianas para la prevención del cibercrimen. Revista Electrónica de Ciencias Penales y Criminalísticas, 13(7), 1-55.

Miró, F. (2012). El cibercrimen fenomenología y criminología de la delincuencia en el ciberespacio. Revista para Análisis del Derecho, 1(1), 1-7.

Montañez, A. (2017). Análisis de los delitos informáticos en el actual sistema penal Colombiano. Tesis de grado, Bogotá, Universidad Libre.

ONU. (2001). Convenio de Ciberdelincuencia. Recuperado de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Pabón, P. (2013). Manual de derecho penal. Bogotá: Ediciones Doctrina y Ley.

Prías, J. (2006). Aproximación al estudio de los delitos informáticos publicado. Revista Derecho Penal, 1(17), 1-10.

Rayón, M. y Gomez, J. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. Anuario Jurídico y Económico Escurialense, 1(47), 209-234.

Recovery Labs. (s.f.). Sobre seguridad informática. Recuperado de: http://www.delitosinformaticos.info/consejos/sobre_seguridad_informatica.html

Riascos, L. (2010). El delito informático contra la intimidad y los datos de la persona en el derecho colombiano. Pasto: Universidad de Nariño.

Rodríguez, J. (s.f.). Análisis de los delitos informáticos presentes en las redes sociales en Colombia para el año 2011 y su regulación. Medellín: Universidad CES.

Sarzana, C. (1979). Criminalità e tecnologia en computers crime. Rassagna Penitenziaria e Criminologia, 1(2), 53.

SEOtop. (2015). Ciberdelitos: definición y tipos más frecuentes. Recuperado de: http://www.seo-posicionamientoweb.com/ciberdelitos-definicion-tipos-frecuentes/

Serrano, E. (2015). La práctica de delitos informáticos en Colombia. Tesis de grado, Bogotá, Universidad Militar Nueva Granada.

Tovar, C. y Amariles, K. (2014). Mitigación de riesgo de delitos informáticos en el contexto empresarial. Tesis de grado, Pereira, Universidad Tecnológica de Pereira.

Anexos

Anexo 1. Ruta metodológica

OBJETIVO GENERAL	OBJETIVOS ESPECÍFICOS	CATEGORÍA	DIMENSIÓN	FUENTE	TÉCNICA	INSTRUMENTO	ITEMS
Análisis documental del delito informático en Cúcuta hurto por medios informáticos y semejantes artículo 269i: (ley 1273/2009)	Establecer algunas de las modalidades de hurtos por medios informáticos y semejantes en transacciones bancarias en personas naturales que se han generado a través de medios informáticos en el Municipio de San José de Cúcuta en el período 2016-2017.	De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos	Involución frente al avance de los delitos informáticos Falta de capacitación de los operadores judiciales para la implementación de esta ley	ley 1273 de 2009 Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia	Técnica de fichaje	Instrumento de investigación documental Matriz de análisis legal	Ficha de diario Ficha de tesis
	Dilucidar el procedimiento penal realizado al delito de hurto por medios informáticos en el Distrito Judicial de Cúcuta en los años 2016-2017.	De los atentados informáticos y otras infracciones	Involución frente al avance de los delitos informáticos Falta de capacitación de los operadores judiciales para la implementación de esta ley	ley 1273 de 2009 Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia	Técnica de fichaje	Instrumento de investigación documental Matriz de análisis legal	Ficha de diario Ficha de tesis
	Exponer posibles soluciones con la finalidad de ser víctima del delito de hurto a través de medios informáticos en el Municipio de San José de Cúcuta.	De los atentados informáticos y otras infracciones	Involución frente al avance de los delitos informáticos Falta de capacitación de los operadores judiciales para la implementación de esta ley	ley 1273 de 2009 Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia	Técnica de fichaje	Instrumento de investigación documental Matriz de análisis legal	Ficha de diario Ficha de tesis

Anexo 2. Formato de instrumentos aplicados

ANÁLISIS DOCUMENTAL DEL DELITO INFORMÁTICO EN CÚCUTA HURTO POR MEDIOS INFORMÁTICOS Y SEMEJANTES ARTÍCULO 269I: (LEY 1273/2009)

Responsables:
William Herney Ariza Salcedo
Mario Adul Villamizar Duran
Luis Gerardo Rodríguez Haro

TECNICA

Análisis documental

Objetivo: Orientar científica e informativamente sobre el hurto por medios informáticos y semejantes en transacciones bancarias en personas naturales en Cúcuta

INSTRUMENTOS

Matriz de análisis legal

Categoria 1

1. Ficha de diarios

1. Nombre del autor : El Congreso de Colombia
2. Título y subtítulo del artículo : "LEY 1273 DE 2009"
3. Título y subtítulo del periódico o revista (subrayado). DIARIO OFICIAL
4. Número del fascículo: Edición 47.223
5. Fecha: Lunes 5 de enero de 2009
6. Número de páginas:2
7. Información: por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se

preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Categoría 2

2. Ficha de tesis.

1. Autor: Zulay Nayiv Sanchez Castillo

2. Título: Análisis de la ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia

3. Tesis: Especialización en seguridad informática

4. Lugar: Universidad Nacional Abierta Y A Distancia —UNADl

6. Fecha: 2017

7. Número de páginas: 140

8. Información: En la actualidad Colombia es víctima, así como muchos países de Latinoamérica de los constantes ataques a la seguridad de la información mediante los diferentes tipos de delitos informáticos conocidos como el sabotaje, los virus, acceso no autorizado a sistemas informáticos, entre otros, los cuales pretenden causar daño a la información como activo vital para las empresas al igual que pérdidas financieras invaluables. Por lo que se ha pretendido hacer frente a esta problemática, a través del diseño e implementación de políticas de seguridad supervisadas y estandarizadas por

organizaciones de calidad internacional, con el fin de mitigar el daño causado por los diferentes delitos informáticos.