ANÁLISIS DE LA LEY 1273 DE 2009 Y LA EVOLUCIÓN DE LA LEY CON RELACIÓN A LOS DELITOS INFORMÁTICOS EN COLOMBIA

ZULAY NAYIV SANCHEZ CASTILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
CHIQUINQUIRÁ
2017

ANÁLISIS DE LA LEY 1273 DE 2009 Y LA EVOLUCIÓN DE LA LEY CON RELACIÓN A LOS DELITOS INFORMÁTICOS EN COLOMBIA

ZULAY NAYIV SANCHEZ CASTILLO

Monografía de investigación para optar el título de especialista en seguridad informática

Director

Salmón González García

Ingeniero de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA “UNAD”
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
CHIQUINQUIRÁ
2017

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Chiquinquirá, 9 de Febrero de 2017

DEDICATORIA

Dedico mi tesis de manera especial a Dios, por darme la sabiduría, confianza, constancia, salud mental y física necesaria para no desfallecer en ningún momento, permitiéndome afianzar los cimientos de mi proyecto de vida profesional al alcanzar el éxito de una meta más en mi camino.

A mi familia, por el ser el pilar de mi vida y estar siempre presentes en cada momento dándome apoyo y depositando su confianza en mí, sin dudar jamás de mis capacidades y habilidades para superar cada reto propuesto y por brindarme siempre el bienestar necesario para alcanzar mis sueños.

AGRADECIMIENTOS

Agradezco el apoyo y colaboración brindada a cada uno de los profesionales académicos de la Universidad Nacional Abierta y a Distancia UNAD que hicieron parte de mi formación, durante el desarrollo de esta especialización por brindarme las herramientas necesarias y fortalecer mis habilidades como profesional, a través de sus conocimientos y enseñanzas.

Agradezco a la Universidad Nacional Abierta y a Distancia UNAD, por permitirme a través de sus programas académicos y la modalidad a distancia, consolidar mi formación profesional y darme herramientas para el desarrollo de mis capacidades intelectuales, éticas y actitudinales en el desempeño de mi vida profesional y en el servicio a la comunidad.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE ANEXOS

Pág.

INTRODUCCIÓN

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.

Las políticas de seguridad informática van siempre de la mano en cada país con la promulgación de leyes estatutarias incluidas en el código penal, en donde se pretende imponer sanciones de tipo penal y económico, a todo tipo de comportamientos ilícitos que traen consigo las nuevas formas de delincuencia cibernética que causa pérdidas económicas y de información.

Teniendo en cuenta lo anteriormente expuesto, se realizará un análisis de la ley 1273 de 2009 denominada "De la protección de la información y de los datos" en Colombia frente a la evolución de los delitos informáticos y su incidencia, finalmente se determinará si dicha ley cumple con el propósito para el cual fue creada.

1. TÍTULO

ANÁLISIS DE LA LEY 1273 DE 2009 Y LA EVOLUCIÓN DE LA LEY CON RELACIÓN A LOS DELITOS INFORMÁTICOS EN COLOMBIA

2. DEFINICIÓN DEL PROBLEMA

En Colombia fue creada la ley 1273 de 2009 denominada "De la protección de la información y de los datos" el 5 de enero de 2009 por el congreso de la república, por la cual se modifica el código penal y se crea un nuevo mecanismo legal, cuyo objetivo es sancionar todo comportamiento ilícito frente a la comisión de los delitos informáticos en el país.

Como ingeniera de sistemas uno de los objetivos es velar por el buen uso y la aplicación de las diferentes políticas de seguridad informática creadas en el país, teniendo en cuenta esto y analizando los 7 años que lleva en ejercicio esta ley sin modificaciones o ajustes que permitan adaptarse a los nuevos escenarios de los delitos informáticos, se pretende presentar las falencias o posibles vacíos legales que permiten el desarrollo y materialización de los mismos, ya que la delincuencia cibernética viene evolucionando y creciendo para adaptarse a las nuevas tendencias tecnológicas utilizadas por los usuarios.

Estos vacíos legales o ambigüedades dentro de la ley 1273 de 2009, permite mostrar como los delincuentes pueden evadir las sanciones penales y económicas, amparados en la falta de instrumentalización de la ley y en la ambigüedad en la definición técnica de los delitos que castiga en algunos de sus artículos.

2.1. FORMULACIÓN DEL PROBLEMA

¿El análisis de la Ley 1273 y la adecuada clasificación de los delitos informáticos ayudarán a la identificación de los vacíos existentes en la legislación nacional, frente a la legislación internacional que contribuya a formular propuestas efectivas para combatir los delitos informáticos?

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Identificar los vacíos existentes en la legislación nacional frente a la legislación internacional por medio del análisis de la ley 1273 y la adecuada clasificación de los delitos informáticos que contribuya a formular propuestas efectivas para combatir los delitos informáticos

3.2. OBJETIVOS ESPECIFICOS

- ✓ Realizar un análisis de la evolución de los delitos informáticos frente al actual marco legislativo internacional y la ley 1273 Colombiana

- ✓ Consultar la legislación contra los delitos informáticos de Argentina, Venezuela y Chile realizando un comparativo frente a la Ley 1273 para determinar las similitudes y diferencias existentes, como punto de referencia a la posible mejora de la legislación colombiana.

- ✓ Realizar un análisis de las sentencias de Ley emitidas en cumplimiento de la Ley 1273 que permita determinar las posibles falencias o ambigüedades de la misma, en busca de mejoras

- ✓ Crear una guía en donde se evidencien propuestas puntuales que contribuyan a mejorar la legislación Colombiana contrarrestando la problemática de seguridad informática y de protección de datos actual

4. JUSTIFICACIÓN

Con la evolución de la tecnología como herramienta para suplir las necesidades del hombre en los diferentes ámbitos, ya sea el hogar, el trabajo, estudio, etc. También aparecen y evolucionan en igual medida las amenazas y los riesgos que colocan en tela de juicio la protección y la intimidad de las personas, sus transacciones y en general la información física y digital que se manipula a diario, provocando que se desencadenen problemas que van más allá de la pérdida de un simple documento por ejemplo o de una clave de cuenta de red social.

Estos problemas de seguridad en la información en la actualidad provocan pérdidas financieras invaluables y numerosos conflictos legales por la materialización de hurtos y fraudes cometidos, esto en el caso de las empresas u organizaciones. Debido a esto desde hace varios años se está luchando contra esta situación para mitigarla y evitarla por medio de la creación o en su debido caso modificación de las herramientas jurídicas concernientes a la normativa de cada país a nivel mundial.

Colombia no es ajeno a esta situación, por lo que desde el año 2009 se modificó el Código Penal en el país y se adicionó en uno de sus títulos una ley estatutaria la cual incluyera la penalización económica y de privación de la libertad de todas aquellas personas o individuos que se valieran de los medios informáticos y telemáticos para atentar contra la integridad, disponibilidad y confidencialidad de la información, entendiendo esta última como un activo primordial en el medio actual y que por ende la pérdida, daño o manipulación inadecuada de la misma puede llegar a causar riesgos financieros o en la reputación entre otros, a las personas y organizaciones.

Por lo anteriormente expuesto, es necesario que las medidas tomadas en las actuales leyes estén acordes y se adapten a las necesidades tecnológicas que están siempre en constante evolución, con el fin de proteger o salvaguardar la información de los diferentes ataques y delitos perpetuados contra la misma, ya que estos últimos están también en constante evolución en cuanto a las técnicas y fines utilizados por los delincuentes para cometer o llevar a feliz término su propósito.

Se observa que Colombia ha sido duramente agobiada en cuanto seguridad de la información se refiere, puesto que cada vez son más los ataques y pérdidas millonarias por la comisión de los delitos informáticos y en este caso teniendo una figura jurídica que a pesar de ser gran ayuda en la penalización de varios de estos delitos, se encuentra también con vacíos legales o llamadas falencias y algunas ambigüedades, que no permiten castigar a las personas o individuos judicializados por dichos delitos, dando así una forma para que estos se escapen de las sanciones promulgadas, basándose en recursos de ley interpuestos en donde demuestran las ambigüedades de la ley que permitan su salida en libertad.

Durante el desarrollo del presente proyecto de investigación dentro del área del conocimiento de la seguridad informática, se pretende realizar un análisis y estudio de la herramienta jurídica creada por el estado colombiano que clasifica y penaliza los diferentes delitos informáticos. Esto con el fin de identificar y establecer con claridad las falencias y/o ambigüedades de la presente ley 1273 de 2009 denominada “De la protección de la información y de los datos”.

Esta tarea de investigación se realiza con la finalidad de ofrecer una serie de medidas que puedan tenerse en cuenta como propuestas puntuales de la mejora de la actual ley, permitiendo de esta forma beneficiar a todos los colombianos, ya sean personas naturales o jurídicas, que buscan mantener la información personal o de sus negocios segura y respaldada por una figura jurídica que permita de forma clara su estricto cumplimiento y posterior castigo justo, a todos aquellos individuos que atenten contra la seguridad de la información en sus diferentes ámbitos.

5. MARCO REFERENCIAL

5.1. ANTECEDENTES

Dentro del estudio los delitos informáticos en Colombia y la aplicación de la actual ley 1273 que penaliza los mismos es necesario tener en cuenta los antecedentes de este fenómeno en el país, de esta manera se logra un mejor análisis de la situación, por lo que se debe tener en cuenta fuentes confiables que permitan la consulta y el avance de la investigación propuesta.

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 el artículo se explican los antecedentes de los delitos informáticos desde el punto de vista general y luego algo más específico enfocado en Colombia. Este artículo de investigación permitirá tener una idea base de los antecedentes de los delitos informáticos en Colombia como parte de la investigación propuesta.

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 muestra de forma clara un estudio socio jurídico de la legislación penal en Colombia referente al cibercrimen o delitos informáticos en el país, al igual que una comparación con la legislación de otros países de tal manera que se pueda tipificar de una manera más clara y precisa los tipos penales previstos dentro de la ley 1273 colombiana. Este ensayo jurídico servirá de guía para el análisis y el comparativo legislativo escogido en el presente proyecto de investigación frente a las leyes jurisprudenciales colombianas.

El artículo de investigación denominado “Aproximación al estudio de los delitos informáticos” publicado por Juan Carlos Prías Bernal Profesor de la Universidad Javeriana (Colombia). Este artículo de investigación explica el estudio realizado a las nuevas tecnologías de información y su incidencia en el derecho penal mostrando que dentro de las actividades tecnológicas actuales algunas de ellas son cobijadas por la legislación penal, pero muchas otras se logran escapar debido a la tipificación realizada. Este artículo de investigación servirá en la

identificación de los vacíos legales existentes en las leyes actuales del derecho penal contra los delitos informáticos.

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). Explica el tratamiento de los delitos en los sistemas de información en el país, especialmente en las empresas las cuales no están preparadas en muchos casos para enfrentar situaciones de este tipo. Este proyecto servirá para el estudio de la evolución de los delitos informáticos en Colombia.

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 se enfoca en los errores cometidos a la hora de la manipulación de herramientas informáticas por parte de los usuarios sin la debida precaución, así como de explicar la necesidad de implementar los controles de seguridad adecuados a cada situación y estar en pleno conocimiento de las normas existentes que protegen la información y su debido uso. Este ensayo servirá para explicar los controles existentes y medidas utilizadas actualmente mediante herramientas jurídicas disponibles en el país para la protección de los datos y la información.

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 de investigación se enfoca en el análisis de los diferentes delitos informáticos que se pueden cometer en las redes sociales existentes dejando en duda la articulación y construcción de la normatividad colombiana y su cumplimiento frente a los mismos. Este artículo de investigación servirá en el proceso de identificar la escasa, errónea o ambigua tipificación de los delitos informáticos en la legislación colombiana.

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). Este proyecto de grado tiene como énfasis la comparación de la legislación colombiana frente a seis países de Latinoamérica en cuanto a delitos informáticos, realiza un

análisis también de los diferentes marcos normativos desde el derecho romano hasta la actualidad. Este proyecto servirá como referencia para realizar el análisis comparativo de la legislación colombiana frente a la internacional.

5.2. *MARCO CONTEXTUAL*

El presente proyecto de investigación se basa en la aplicación de la ley y los delitos informáticos en Colombia, en donde el 5 de enero de 2009 fue publicada la Ley 1273 más conocida como la "Ley de Delitos Informáticos", esta tuvo sus primeros antecedentes históricos veinte años atrás en la legislación colombiana con el Decreto 1360 de 1989 en el cual es reglamentada la inscripción del software o soporte lógico en el Registro Nacional de Derecho de Autor, lo que sirvió para aquellas personas que se vieron afectadas por la violación al derecho de autor. A partir de este momento se tuvo fundamento para proteger la propiedad intelectual y las nuevas creaciones de software y otras soluciones que tuvieran que ver con la informática o desarrollo de nuevas tecnologías.

Mediante lo consagrado en este decreto reglamentario de la inscripción del soporte lógico y así mismo en los artículos 51 y 52 del Capítulo IV de la Ley 44 de 1993 sobre derechos de autor, se constituyen en Colombia como las primeras normas que sancionan los delitos contra derechos de autor 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."[1]

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.*

[1] Ley 599 de 2000 disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

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.[2]

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.

De igual manera, en ese mismo año el 5 de enero aparece un nuevo bien jurídico la Ley 1273 de 2009, la cual hace parte del complemento y modificación realizada al Código penal colombiano y nace con el objeto de la protección de la información y los datos, por medio de la cual se preserva los sistemas de información y las comunicaciones. Esta ley se divide en dos capítulos, de los cuales en el primero de ellos se establece las medidas para la protección de la confidencialidad, integridad y disponibilidad de la información y en el segundo capítulo que la compone hace referencia a otras infracciones y los atentados informáticos.

Con la aparición de este bien jurídico, se tipificaron los delitos informáticos en Colombia de la siguiente manera:

Acceso abusivo a un sistema informático (modificado del Código Penal); obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios web para capturar datos personales y transferencia no consentida de activos.

[2] Ley 599 de 2000 Libro II, Capitulo VII disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

Con este marco legislativo, Colombia ingresa a la lista de países en el mundo que buscan proteger la información y contrarrestar la problemática de seguridad informática a nivel general, convirtiéndose de esta manera en un punto de referencia importante para las entidades privadas y públicas del país respecto a la creación de políticas, procedimientos y planes de mejora en seguridad de la información frente a los delitos informáticos y por su parte sirve de guía en las acciones penales que se pueden adelantar contra las personas que incurran en estas acciones delictivas.

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.

- 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 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.

- 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 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.

Este tipo de situaciones delictivas son bastante frecuentes desde hace varios años y a pesar de las recomendaciones de no emitir este tipo de mensajes que atentan contra la intimidad de la persona, ha sido bastante difícil la concientización de las personas frente a este fenómeno creciente y más aun con el auge de las redes sociales y sus medios de comunicación que cada vez son mas versátiles.

5.3. MARCO TEÓRICO

5.3.1. ***Delitos Informáticos.*** Desde hace muchos años se viene trabajando el concepto de delito informático o delito electrónico, puesto que el avance tecnológico es imparable, así mismo las nuevas formas de delinquir evolucionan y con ellas los problemas de protección de la información de las personas del

común y de las organizaciones o empresas a nivel nacional e internacional. De acuerdo a esto, diversos expertos en el campo de la informática y también del derecho penal así como el informático han dando sus puntos de vista sobre el concepto de delito informático así:

Según el experto italiano Carlos Sarzana 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*”*[3]

María de la Luz Lima 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*"*[4]

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*"*.[5]

5.3.2. ***Tipos de delitos informáticos.*** En el año 2001 en la ciudad de Budapest se llevó a cabo el primer congreso contra la cibercriminalidad, en este proceso intervinieron los países asociados a la ONU (Organización de la Naciones Unidas) en donde se promulgó un convenio o tratado que busca identificar, tipificar y establecer un conjunto de normas contra la delincuencia cibernética o delitos informáticos a nivel internacional como modelo a tratarse en cada país, con el fin de mitigar los efectos adversos de este tipo de acciones ilegales en contra de

[3] Asociación Argentina De Derecho De Alta Tecnología. Delitos Informáticos Antecedentes Internacionales para una Legislación Nacional Proyectos Legislativos Recuperado de: http://www.aadat.org/delitos_informaticos20.htm

[4] Asociación Argentina De Derecho De Alta Tecnología. Delitos Informáticos Antecedentes Internacionales para una Legislación Nacional Proyectos Legislativos Recuperado de: http://www.aadat.org/delitos_informaticos20.htm

[5] TELLEZ VALDÉS, Julio. “Los Delitos informáticos. Situación en México”, Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996

los bienes tanto económicos como morales a los que se ven expuestos las personas actualmente con el uso de la tecnóloga en cada ámbito.

Por esta razón y a pesar que existen fuentes diversas que tipifican esta clase de delincuencia o acciones delictivas contra la información, 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:[6]

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.

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

[6]Council of Europe, (2016).Convention on Cybercrim CETS No.: 185.Recuperado de http://www.coe.int/es/web/conventions/home

5.3.3. *Evolución de los delitos informáticos*. 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, sino también por la gran importancia de las telecomunicaciones, 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.

Esta expansión tiene grandes beneficios en la actualidad, puesto que ahora las grandes empresas y en cada hogar existe un aparato electrónico con conexión a la red de redes "internet" lo que permite la transmisión de información con mas facilidad, pero al mismo tiempo supone un peligro a la misma, ya que estará expuesta a diversas amenazas contra su integridad, disponibilidad y confidencialidad.

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 esta situación y entrando en la actualidad, a partir de los años 90's y hasta la fecha la comisión de delitos informáticos ha ido en aumento y han aparecido nuevas tipologías como por ejemplo la pornografía infantil, phising o ingeniería social, acceso abusivo a la información, daño, uso de software malicioso, entre otros.

Por tal razón, ya se han clasificado específicamente dentro de las legislaciones internacionales para darles un tratamiento adecuado, en donde se han definido las características de los mismos, su forma de materializarse y las sanciones a aquellas personas que incurran en su comisión.

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 cual tiene por objeto dar disposiciones legales para el tratamiento y sanción a todas las acciones que tuviesen que ver con la ciberdelincuencia, sirviendo de esta manera como primer marco legislativo para todas las naciones, como parte de la estrategia de prevención y acciones contra esta situación. Este convenio no ha tenido ninguna actualización o modificación a la fecha.

5.3.4. ***Delitos informáticos tipificados en Colombia***. En Colombia dentro del marco legal establecido el 5 de Enero de 2009 mediante la Ley 1273, se realizó un trabajo de tipificación o clasificación de los delitos informáticos en donde de acuerdo a su comisión se denotan de la siguiente manera:

5.3.4.1. ***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.*[7]

De acuerdo a este concepto se considera de gran importancia incluir este delito por el alto grado de riesgo que el mismo representa para cualquier sistema de una

[7] Posada Maya, R. (2006b). Aproximación a la criminalidad informática en Colombia. Revista de derecho, comunicaciones y nuevas tecnologías (2), págs 11-60

organización o empresa, debido a que si se llega a materializar la acción de intrusión se pone en riesgo toda aquella información que pueda llegar a considerarse como vital para el ejercicio o desarrollo de labores de la organización. Por esta razón en 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 […]"[8]

5.3.4.2. ***Obstaculización ilegítima de sistema informático o red de telecomunicación***. Este delito tiene que ver con el uso de diferentes herramientas empleadas por un hacker o delincuente cibernético para interrumpir las funciones normales de un sistema, con el fin de conseguir un beneficio como robo o borrado de información o en algunos casos realizar un daño a gran escala denegando los servicios de red o telemáticos, en donde la organización no tenga comunicación interna ni externa lo que implica pérdidas millonarias, esto se debe a la parálisis del normal funcionamiento de la empresa hasta lograr una solución que permita retomarla.

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"[9]

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 […]"[10]

5.3.4.3. ***Interceptación de datos informáticos***. Este tipo de delito se comisiona cuando el delincuente intenta o accede a una parte de un sistema o por

[8] Ley 1273 de 2009 Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492
[9] CERT. (2001) Denial of Service Attacks. Software Engineering Institute. Carnegie Mellon. Disponible en: www.cert.org/tech_tips/denial_of_service.html
[10] Ley 1273 de 2009 Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

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 269C 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 […]"[11].

5.3.4.4. ***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 […]"[12]

5.3.4.5. ***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

[11] Ley 1273 de 2009 Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492
[12] Ley 1273 de 2009. Artículo 269D Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

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 […]"[13]

5.3.4.6. *Violación de datos personales*. 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."[14]

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"[15]

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

---

[13] Ley 1273 de 2009. Artículo 269E Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[14] Manent, M. Derecho.com. Violación de datos personales disponible en: http://www.derecho.com/c/Violaci%C3%B3n_de_datos_personales

[15] Ley estatutaria 1581 de 2012. Artículo 3, Cap. I disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

"[…] 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 […]"[16]

5.3.4.7. ***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 […]"[17]

5.3.4.8. ***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

[16] Ley 1273 de 2009. Artículo 269E Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[17] Ley 1273 de 2009. Artículo 269G Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

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”[18]

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 […]”[19]

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

5.3.4.9. ***Transferencia no consentida de activos***. Este delito hace referencia a la modalidad de hurto o estafa, puesto que los delincuentes se basan en el uso de diferentes herramientas y tácticas para cometer hechos delictivos que les permitan apoderarse de manera no consentida de activos que afectan al patrimonio económico de la victima, ejemplo de este tipo de delito es el robo o clonación de las claves de las tarjetas de crédito y el hurto de las contraseñas de cuentas bancarias, con las cuales el criminal a través de internet o los diversos servicios bancarios que ofrecen las entidades realiza transferencias de la cuenta de la victima a su cuenta personal en varias transacciones, que son similares al denominado pitufeo con el fin de no ser descubiertos.

Este tipo de delito es también contemplado dentro del código penal, debido a que hace parte de la tipificación de hurto y ya en ampliación e individualización del tema se describe en la Ley 1273 de 2009 en el artículo 269J como “El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave”[20]

5.3.5. ***Evolución de la legislación Colombiana***. Con el auge de la informática y las telecomunicaciones desde su origen, cada día es una lucha continua por defender el derecho a la intimidad, el acceso a la información y el buen uso de la misma. Por esta razón cada país vela por el cumplimiento de estos

[18] Ley 599 de 2000. Artículo 239, Titulo VII, Cp I disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

[19] Ley 1273 de 2009. Artículo 269I Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

[20] Ley 1273 de 2009. Artículo 269J disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

aspectos a través de sus marcos legislativos, promulgando leyes que permitan brindar seguridad a toda la comunidad, debido a que de la misma manera como avanza la tecnología y las comunicaciones así mismo lo hace la delincuencia, este es un ámbito cambiante, en donde debe encontrarse la forma de acoplarse e ir avanzando en instrumentos jurídicos que contemplen las diversas situaciones.

De esta manera dentro de las normas y marcos jurídicos colombianos se han dispuesto herramientas que buscan proteger el acceso a la información, almacenamiento, recolección, registro y transmisión de la misma, así como la protección de la intimidad. Dentro de estos marcos esta el ámbito de derecho público y el derecho punitivo los cuales han ido evolucionando.

5.3.5.1. ***Derechos fundamentales de acceso a la información, habeas data, derecho a la intimidad y protección de datos***. 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"[21]

A este artículo se le une, la Ley 57 de 1985 en su Capitulo II denominado "Acceso ciudadano a los documentos"[22], 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, cuidando la debida reserva si a ello hubiese lugar de acuerdo a la normativa y la constitución colombiana sobre la clasificación de la información.

[21] Constitución política de Colombia. Artículo 15 disponible en http://www.constitucioncolombia.com/titulo-2/capitulo-1/articulo-15

[22] Ley 57 de 1985. Capitulo II recuperado de: http://www.archivogeneral.gov.co/sites/all/themes/nevia/PDF/Transparencia/LEY_57_DE_1985.pdf

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”[23]

- 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 [24]

- 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.[25]

- La Ley 599 y 600 de 2000, Códigos Penal y Procesal Penal Colombiano[26]

- 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[27]

- 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.[28]

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.[29]

5.3.6. ***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

[23] Código contencioso administrativo disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6543
[24] Ley 44 de 1993 disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3429
[25] Ley 527 de 199 disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276
[26] Ley 599 de 2000 disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html y Ley 600 de 2000 disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6389
[27] Ley 1266 de 2008 disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488
[28] Ley 1581 de 2012 disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981
[29] Ley 1273 de 2009 Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

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.

Gracias a este primer paso en el año 2001, se dió un tratamiento penal para la protección y cumplimiento de estos derechos mediante la creación de la "Ley especial contra los delitos informáticos", la cual consagra la nueva tipificación realizada a esta problemática y deroga la antigua ley de protección a la privacidad de las comunicaciones.

Dentro de esta ley se denotan los delitos informáticos como:

5.3.6.1. ***Acceso indebido***. En este se hace referencia al acceso a cualquier sistema informático sin la debida autorización o la interceptación del mismo. De acuerdo a esto, la ley lo cita de la siguiente manera "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 […]" [30]

5.3.6.2. ***Sabotaje o daño a sistemas***. Dentro de este delito se hace referencia al uso de software, hardware o cualquier componente tecnológico que pueda causar daño a la información, atentando directamente contra la integridad y disponibilidad de la misma. En este caso la ley especial enuncia este delito como "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"[31]

5.3.6.3. ***Favorecimiento culposo del sabotaje o daño***. En este caso se hace una alusión clara a la comisión del delito descrito en el numeral anterior por negligencia o imprudencia lo que inculparía también a aquellas personas que ayuden a cometer el ilícito, lo que la ley cita como "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"[32]

5.3.6.4. ***Acceso indebido o sabotaje a sistemas protegidos***. Cuando se habla de sistemas protegidos, se debe pensar en aquellos sistemas informáticos que contienen información confidencial relacionada con el patrimonio de las

[30] [29] [30] Gaceta Oficial de la república bolivariana de Venezuela (2001). Ley especial contra los delitos informáticos Recuperado de: http://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

personas naturales o jurídicas y que para el caso de Venezuela también se considera sistema protegido los sistemas de función pública y todo atentado contra los mismos es catalogado como delito informático, debido a las herramientas y tácticas utilizadas de sabotaje y alteración de la información.

5.3.6.5. ***Posesión de equipos o prestación de servicios de sabotaje***. Realmente la preocupación por la protección de la información, lleva a intentar abarcar todos los aspectos y dentro de este pensamiento se encuentra la acción de consagrar como delito a todo aquel que preste, distribuya o colabore mediante el uso de software malicioso a realizar un ataque contra la seguridad de los sistemas informáticos, con el fin de sustraer o dañar información. En este aspecto la ley especial contra delitos informáticos venezolana es enfática y lo cita de la siguiente manera:

"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 […]"[33]

5.3.6.6. ***Espionaje informático***. Este delito tiene que ver con la obtención de información mediante el uso de herramientas como por ejemplo los spywares, los cuales permiten obtener información a través de la intrusión en un sistema recepcionando información y enviándola al delincuente quien se encarga de usarla en beneficio propio mediante su divulgación o realizando algún tipo de extorsión con la misma a la víctima. Frente a este problema la ley venezolana es clara y en su artículo 11 de la Ley especial contra delitos informáticos señala este delito como "Toda persona que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualesquiera de sus componentes […]" [34]

5.3.6.7. ***Falsificación de documentos***. Debido a que uno de los delitos más comunes es la alteración o en algunos casos falsificación de información con el fin de conseguir beneficios económicos y/o de reconocimiento a nivel laboral o en otros ámbitos, en Venezuela se tipificó esta acción delictiva como parte de los delitos informáticos, puesto que se requiere castigar a las personas que lleven a cabo el ilícito valiéndose de medios informáticos o telemáticos. Por esta razón la ley venezolana en su artículo 12 de la ley especial contra los delitos informáticos lo consagra como "Quien, a través de cualquier medio, cree, modifique o elimine un

[33] [32] [33] Gaceta Oficial de la república bolivariana de Venezuela (2001). Ley especial contra los delitos informáticos Recuperado de: http://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

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 […]"[35]

5.3.6.8. ***Hurto***. Como ya se ha descrito antes en este documento el hurto es una de las acciones delictivas en donde el delincuente pretende apoderarse de bienes materiales o digitales sin utilizar la violencia o intimidación, y es catalogado como un hecho punible castigado en todas las naciones dentro de sus códigos penales y constituciones y en Venezuela no es la excepción, en donde se hace referencia al mismo en este caso en el artículo 13 de la ley especial contra delitos informáticos de la siguiente manera:

"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 […]"[36]

5.3.6.9. ***Fraude***. Se entiende por fraude toda acción que ejerza una persona de manera incorrecta o ilegal, con el objetivo de obtener un beneficio económico, político o de cualquier otra índole. Este tipo de delito es muy común en la sociedad y es una forma de corrupción dentro de las entidades u organizaciones.

Existen varias formas de fraude y una de ellas es a través de sistemas informáticos o mediante el uso de elementos electrónicos, por esta razón en Venezuela se tipifica también como parte de los delitos informáticos y dentro de la ley especial contra delitos informáticos se enuncia de la siguiente manera:

"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 […]"[37]

5.3.6.10. ***Manejo fraudulento y apropiación de tarjetas inteligentes o instrumentos análogos***. Este delito es muy importante, debido a que se comete casi que a diario, cuando se da a conocer en noticieros locales, periódicos

[36] [35] Gaceta Oficial de la república bolivariana de Venezuela (2001). Ley especial contra los delitos informáticos Recuperado de: http://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

o noticieros nacionales que han robado altas sumas de dinero mediante la clonación de las tarjetas de crédito, la utilización de herramientas tecnológicas dispuestas y adaptadas a las necesidades del delincuente quien las emplea en los cajeros automáticos de las entidades financieras y espera el momento preciso que ingrese una víctima a realizar una transacción para duplicar la banda magnética de la tarjeta y con esa información poder realizar transacciones de las cuentas de las victimas a su cuenta personal a través de internet o en otros casos realizar la reproducción de la misma, con el fin de hacer efectivos retiros en diferentes puntos para no ser atrapado.

En este caso la ley venezolana consagra este delito dentro de su ley especial contra los delitos informáticos en el artículo 16 como "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 […]"[38] 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 […]"[39]

5.3.6.11. *Provisión indebida de bienes o servicios y posesión de equipo para falsificaciones*. Con el uso dado a los delitos de fraude, manejo y apropiación fraudulenta de tarjetas y/o instrumentos análogos, el gobierno venezolano busca cubrir todas las áreas sin dejar ningún detalle por fuera. Por esta razón, es tan enfático en sancionar no solamente a las personas que cometan el delito en sí, sino que también a todas aquellas personas que sirvan de soporte y cuartada para cometerlo.

De acuerdo a lo expuesto anteriormente dentro de la ley especial contra los delitos informáticos, existen los artículos 18 y 19 que hacen un énfasis en este tipo de conductas de provisión indebida de bienes o servicios y posesión de equipo para falsificaciones, las sanciones dispuestas van desde multas económicas hasta pérdida de la libertad por el tiempo establecido en la presente ley.

[38] [37] Gaceta Oficial de la república bolivariana de Venezuela (2001). Ley especial contra los delitos informáticos Recuperado de: http://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

5.3.6.12. ***Violación a la privacidad.*** Este tema es bastante importante no sólo en la legislación venezolana sino a nivel mundial, es por eso que cada país busca implementar herramientas que permitan el control de la información, el acceso a la misma y proteger la privacidad de las personas, por lo que este tema es ampliamente expuesto dentro de esta 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.

5.3.6.13. ***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.

5.3.6.14. ***Propiedad intelectual y oferta engañosa***. Los derechos de autor y la violación a la propiedad intelectual siempre han sido vulnerados con el auge de delitos como la piratería, que busca un lucro frente a la copia y distribución de material fidedigno, perjudicando de esta forma a los autores originales de las obras ya sean musicales, aplicaciones, entre otras.

Por otro lado, también se destaca la publicidad u oferta engañosa como delito informático en este país, haciendo referencia a todos aquellos mensajes tipo spam en los correos electrónicos o por otros medios telemáticos y electrónicos, en donde se divulgue información no cierta o dudosa y en forma masiva.

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.

5.3.7. ***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. Por lo que dentro de su código penal no fueron consagrados aquellos hechos delictivos que tuvieran que ver con este tema.
Con el auge de la tecnología y a su vez con el avance de la delincuencia informática se vio la necesidad de modificar el código penal y crear nuevos instrumentos jurídicos que dieran respuesta a esta problemática de orden mundial. Respaldando este aspecto fueron promulgadas leyes que comprendieran temas como la protección de datos, la privacidad, la propiedad intelectual, promoción de la industria del software y por último los delitos informáticos y ciberseguridad.

5.3.7.1. ***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, se hace alusión a al protección de datos y también se consagran aspectos como derechos, uso y responsables del registro de datos, así como también se sancionan de manera penal y económica todos los hechos delictivos en contra de estos dos temas.

Por otro lado, también se encuentra la Ley 24.766, sancionada y promulgada en diciembre de 1996, por medio de la cual se sancionan y se describen las disposiciones legales contra la confidencialidad de la información.

5.3.7.2. ***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.

5.3.7.3. ***Promoción de la industria del software***. Realmente la legislación Argentina frente a este tema es innovadora, ya que en ninguna otra legislación se trata la promoción, distribución y creación de software como una temática individual, la cual requiere protección con la delincuencia informática o ciberdelincuencia, en este aspecto este país latinoamericano sanciona y promulga dos leyes en favor de la protección del software y lo considera como actividad productiva de transmisión asimilable a una actividad industrial.

Teniendo en cuenta esta clasificación dada al 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.

5.3.7.4. ***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, la privacidad, alteración, destrucción, manipulación y empleo de cualquier medio por el cual se afecte la integridad, confidencialidad y disponibilidad de la información en cualquier ámbito.

5.3.8. ***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.

5.3.8.1. ***Propiedad intelectual***. En este aspecto Chile promulgo la ley 17.336 del 2 de octubre de 1970[40], la cual protege los derechos de autor, la moral y establece sanciones y disposiciones legales para cubrir las necesidades jurídicas frente a este tema. Esta ley desde su promulgación ha tenido cinco versiones y su última versión y modificación fue sancionada el 29 de mayo de 2014, lo que permite tener una mayor aplicación y se adecúa a las situaciones cambiantes de este país.

5.3.8.2. ***Protección de datos***. Con relación a la protección de datos de carácter personal, se promulga la Ley 19.628 denominada “Protección de datos de

[40] Ley 17.366 de 1970 Propiedad intelectual disponible en: http://www.leychile.cl/Navegar?idNorma=28933

carácter personal"[41] 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 (económico, comercial, financiero, público, etc.) y se establecen los derechos de los titulares frente al tratamiento que se le de por parte de los diferentes organismos o entidades a los mismos.

5.3.8.3. ***Delitos informáticos***. El 7 de junio de 1993 fue publicada la Ley 19.223 denominada "Ley relativa a delitos informáticos"[42], en donde se tipifican figuras penales relativas al uso de la informática. Esta ley nace de la necesidad de establecer un bien jurídico que abracara delitos especiales que difieren en características de las conductivas delictivas tradicionales consagradas en el código penal chileno. 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.

5.3.8.4. ***Documento electrónico***. Chile ampara la creación, registro, comercialización y uso de las firmas electrónicas, documentos electrónicos y los servicios de certificación, los cuales son también vulnerables con el uso masivo de las nuevas tecnologías que son usadas para el robo, daño e interceptación de la información colocando en riesgo su integridad, confidencialidad y disponibilidad en este caso en todas aquellas situaciones que requieran de la realización de transacciones con documentos autenticados mediante el uso de firmas o certificados electrónicos.

Atendiendo a estas necesidades se crea la Ley 19.799 denominada "Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma"[43], 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.

5.3.9. ***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):

[41] Ley 19.628 Protección de datos de carácter personal disponible en: http://www.leychile.cl/Navegar?idNorma=141599

[42] Ley 19.223 Ley Relativa a delitos informáticos disponible en: http://www.leychile.cl/Navegar?idNorma=30590

[43] Ley 19.799 Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma disponible en: http://www.leychile.cl/Navegar?idNorma=196640

*"*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.*"*[44]

De acuerdo a esto, se entiende la seguridad de la información como uno de los temas más preocupantes actualmente, ya que la información se ha convertido en un activo primordial para las organizaciones o empresas y en general para todo el mundo, por lo que la misma debe conservar siempre sus tres principios básicos ser confidencial, integra y disponible. 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.*[45]

5.4. MARCO CONCEPTUAL

- Ley: Es una norma o una regla que nos dice cuál es la forma en la que debemos comportarnos o actuar en la sociedad. Las Leyes nos dicen lo que es permitido y lo que es prohibido hacer en Colombia; así si todos las cumplimos podríamos lograr que existan menos conflictos en la población. Traen soluciones Evitan conflictos.[46]

- Legislación: Se denomina legislación, por una parte a todo el conjunto de leyes que existen en un Estado y que regulan los comportamientos de los individuos pertenecientes al territorio de un país. En este sentido, consiste en todo el ordenamiento jurídico, todo el sistema o conjunto de normas que pueden

[44] Gobierno de España. Ministerio de educación, cultura y deporte. MONOGRÁFICO: Introducción a la seguridad informática - Seguridad de la información / Seguridad informática. Seguridad de la información / Seguridad informática Recuperado de: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

[45] Carhuamaca, D. Seguridad de la información: realidad o Utopia Recuperado de: http://www.monografias.com/trabajos85/seguridad-informacion-realidad-o-utopia/seguridad-informacion-realidad-o-utopia.shtml#ixzz43P7fBC32

[46] Congreso de la República de Colombia. ¿Qué es una ley? Recuperado de: http://www.senado.gov.co/legales/item/11164-que-es-una-ley

encontrarse en un país, y que responden a un sistema jurídico específico, entendiendo a éste último como todo el conjunto de instituciones del gobierno, las normas, las creencias y las concepciones sobre lo que se considera "derecho", cuál debería ser su función y las maneras de aplicarlo, perfeccionarlo, enseñarlo y estudiarlo en dicha sociedad determinada.[47]

- Derecho penal: Es la rama del derecho que establece y regula el castigo de los crímenes o delitos, a través de la imposición de ciertas penas [48]

- Cibercrimen: Acceder sin previo consentimiento a la información y datos que son propiedad de personas, empresas o gobiernos. Unos ataques que nunca suceden de forma física, si no que siempre se llevan a cabo de forma virtual.[49]

- Confidencialidad: Se entiende en el ámbito de la Seguridad Informática como la protección de datos y de información intercambiada entre un emisor y uno o más destinatarios frente a terceros.[50]

- Integridad: En la Seguridad Informática, la Integridad es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.[51]

- Disponibilidad: Se refiere a la seguridad que la información pueda ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.[52]

- Autenticidad: Este pilar se define aquella información legítima, que al ser interceptada, puede ser copiada de su formato original a pesar de que la información sea idéntica[53]

- Amenaza: Una amenaza informática es un posible peligro del sistema. Puede ser una persona (cracker), un programa (virus, caballo de Troya, etc.), o un

[47] Definición. Definición de legislación Recuperado de: http://definicion.mx/legislacion/

[48] Definición de derecho penal - Qué es, Significado y Concepto http://definicion.de/derecho-penal/#ixzz43PVvmiEK

[49] Abogados Portaley Madrid penal, civil e Internet (2015). Qué es y como combatir el cibercrimen Recuperado de: http://portaley.com/2015/04/que-es-y-como-combatir-el-cibercrimen/#

[50] Guzmán, A. (2011). Seguridad Informática. Confidencialidad e integridad Recuperado de: http://seguridadanggie.blogspot.com.co/2011/11/confidencialidad.html

[51] Guzmán, A. (2011). Seguridad Informática. Confidencialidad e integridad Recuperado de: http://seguridadanggie.blogspot.com.co/2011/11/confidencialidad.html

[52] Bradanovic, T. Conceptos Básicos de Seguridad Informática Recuperado de: http://www.bradanovic.cl/pcasual/ayuda3.html

[53] Universidad Nacional Abierta y a Distancia. Dateca. Sistema de gestión de la seguridad de la información 1.1 Lección 1: Pilares de la seguridad informática Recuperado de http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/11_leccin_1_pilares_de_la_seguridad_informtica.html

suceso natural o de otra índole (fuego, inundación, etc.). Representan los posibles atacantes o factores que aprovechan las debilidades del sistema[54]

- Riesgo: Es una condición del mundo real, en el cual hay una exposición a la adversidad, conformada por una combinación de circunstancias del entorno, donde hay posibilidad de perdidas[55]

- Seguridad: Es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático[56]
- Información: Está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente[57]

- Vulnerabilidad: Es el punto o aspecto del sistema que es susceptible de ser atacado o de dañar la seguridad del mismo. Representan las debilidades o aspectos falibles o atacables en el sistema informático[58]

- TIC: Nuevas tecnologías de la información y comunicación empleadas para la transmisión de contenidos a través de internet, las cuales funcionan como medios y aplicaciones en el desarrollo de las actividades de los individuos. Gracias a estas, los campos de la educación, cultura, política, opinión y demás han logrado avanzar en la distribución y masificación de sus contenidos, planes de acción y trabajo y las diversas funcionalidades en sus áreas.[59]

- Aplicaciones: Programa o herramienta que puede descargarse a través de un dispositivo móvil como smartphones o tablets. Para la descarga de ellas es necesaria la conexión a Internet y pueden ser gratuitas o pagas.[60]

- Red: Conjunto de equipos y dispositivos periféricos conectados entre sí. Se debe tener en cuenta que la red más pequeña posible está conformada por dos equipos conectados.[61]

---

[54] Universidad Nacional Abierta y a Distancia. Dateca. Riesgos y control informático. Lección 1: Conceptos de Vulnerabilidad, Riesgo y Amenaza recuperado de http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html

[55] Universidad Nacional Abierta y a Distancia. Dateca. Riesgos y control informático. Lección 2: Clasificación de los riesgos recuperado de http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html

[56] Definición de seguridad informática - Qué es, Significado y Concepto Recuperado de http://definicion.de/seguridad-informatica/#ixzz4KwYk9v7j

[57] Concepto de información - Definición, Significado y Qué es Recuperado de http://definicion.de/informacion/#ixzz4KwcV6NZq

[58] Universidad Nacional Abierta y a Distancia. Dateca. Riesgos y control informático. Lección 1: Conceptos de Vulnerabilidad, Riesgo y Amenaza recuperado de http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_1_conceptos_de_vulnerabilidad_riesgo_y_amenaza.html

[59] [60] Colombia digital. Conceptos TIC Recuperado de https://colombiadigital.net/actualidad/articulos-informativos/conceptos-tic.html

[61] CCM (2016). El concepto de red Recuperado de http://es.ccm.net/contents/252-el-concepto-de-red

- Red social: es una estructura virtual que proporciona interactividad constante entre los usuarios, quienes comparten distintos intereses y relaciones en común. A través de este espacio se promueve la comunicación y participación de los cibernautas desde la publicación de imágenes, videos, links de referencias o contenidos de su interés[62]

5.5. MARCO LEGAL

En Colombia los diferentes delitos informáticos se sancionan 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:[63]

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.

Por otro lado existen leyes que regulan en el país la protección de datos personales, propiedad intelectual y se dictan disposiciones sobre el uso o la manipulación de la información o datos por medios electrónicos. Dentro de estas leyes están:

[62] Colombia digital. Conceptos TIC Recuperado de https://colombiadigital.net/actualidad/articulos-informativos/conceptos-tic.html

[63] Ley 1273 de 2009 Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

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

La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada.[64]

- 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.

Esta ley en principio tiene el mismo objeto que la ley estatutaria 1581 de 2012, la diferencia entre estas dos leyes radica en que la ley 1266 sólo establece parámetros y regulaciones para el derecho de Hábeas Data para datos de carácter financiero y crediticio, mientras que la ley 1581 hace referencia a todas aquellas bases de datos que almacenen y utilicen datos personales con excepción de las bases de datos de uso doméstico, de inteligencia, de seguridad nacional, de estadísticas de censos y aquellas que hacen referencia al ámbito periodístico.[65]

- 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:

[64] Ley 1581 de 2012 disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981
[65] Ley 1266 de 2008 disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

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

Esta ley se divide en dos partes en donde se refiere al uso de la información o datos para el comercio electrónico, firmas digitales, mensajes de dato por medio escrito y digital, la certificación de las personas naturales y jurídicas para realizar transacciones electrónicas, pero así mismo esta ley proporciona reconocimiento legal a los documentos electrónicos tal como se haría con los documentos físicos y por otro lado los admite como prueba en un proceso legal.[66]

- 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.[67]

- 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 donde se dan regulaciones para la protección intelectual y los derechos de autor en general y se adicionan nuevas disposiciones como el soporte lógico (Software), en donde se toma de acuerdo a lo descrito en el artículo 3 de la Decisión Andina 351 de 1993, puesto que en la ley 23 de 1982 no se encontraba estipulado.[68]

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

[66] Ley 527 de 199 disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276
[67] Ley 23 de 1982 disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3431
[68] Ley 44 de 1993 disponible en: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3429

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:[69]

- ✓ 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 le 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” emitida el 28 de Mayo de 1993 y que entro en vigencia el 7 de Junio del mismo año y que sanciona los delitos informáticos de la siguiente manera: [70]

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.

[69] Ley 26.388 Recuperado de: http://infoleg.mecon.gov.ar/infolegInternet/verNorma.do?id=141790
[70] Ley 19223 de Chile Recuperado de: http://www.leychile.cl/Navegar?idNorma=30590

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 ultimo 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: [71]

Titulo II – De los delitos. Capitulo 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

[71] Ley especial contra los delitos informáticos Recuperado de: http://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

- ✓ 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.

6. DISEÑO METODOLÓGICO

6.1. TIPO DE INVESTIGACIÓN

El presente proyecto es una monografía de investigación, debido a que es un tema en desarrollo y no hay una línea base de investigación sobre el tema escogido. Se presentará mediante un enfoque cualitativo, ya que se estudiará y analizará material bibliográfico que permita resolver la pregunta de investigación formulada.

En este caso se hará un análisis de la ley 1273 de 2009 Colombiana y se realizará un comparativo de la misma frente a la legislación de los países escogidos Argentina, Venezuela y Chile, con el fin de definir falencias en la herramienta jurídica de Colombia y presentar una guía con propuestas puntuales que contribuyan a mejorar la legislación actual, encaminándose a una forma más efectiva de contrarrestar los problemas de seguridad informática y de protección de datos.

6.2. DISEÑO DE INVESTIGACIÓN

Para la realización de este proyecto se tomará como herramienta de recolección y análisis de información; el análisis documental, ya que por medio del mismo se pretende estudiar y analizar a fondo la problemática basándose en las normas legislativas existentes que hacen referencia al tema en cuestión (ley 1273 de 2009 de Colombia, la ley 19223 de Chile, la ley 26.388 Argentina, la ley especial contra delitos informáticos de Venezuela, el convenio contra el cibercirmen de Budapest), que serán utilizadas como base para la realización del comparativo legislativo que permita obtener los resultados propuestos.

De acuerdo a esto, se utilizará fuentes de recolección de información secundarias, como material bibliográfico que permita determinar la evolución de los delitos informáticos en Colombia y la aplicación de la ley, por medio de las investigaciones, estudios y tesis publicadas que tienen relación con el tema en mención. Permitiendo de esta forma hacer un análisis a la información encontrada que pueda mostrarse como parte de la hipótesis planteada en el proyecto a ejecutar.

6.3. POBLACIÓN

Para este proyecto la población esta constituida por la clasificación de los delitos informáticos tipificados en Colombia, estos son:

- Acceso abusivo a un sistema informático
- Obstaculización ilegítima de sistema informático o red de telecomunicación
- Interceptación de datos informáticos
- Daño Informático
- Uso de software malicioso
- Violación de datos personales
- Suplantación de sitios web para capturar datos personales
- Hurto por medios informáticos y semejantes
- Transferencia no consentida de activos

6.4. MUESTRA

Es de carácter cuantitativo, ya que será tomada de los diferentes informes en donde se puede contabilizar el nivel de ocurrencia de los delitos informáticos en Colombia, de los cuales se tomarán como referencia los que se presentan con mayor fuerza actualmente en el país, estos son: violación de datos personales y hurto por medios informáticos.

6.5. METODOLOGIA DE DESARROLLO

Para lograr cumplir con los objetivos de la presente monografía de investigación, es necesario realizar las siguientes actividades:

- ✓ Se tomará el Convenio de Budapest como normativa que permita tener determinado cuales son los delitos informáticos tipificados y aceptados a nivel internacional, puesto que esto servirá como base de la investigación para la resolución del problema formulado.

- ✓ Se realizará un comparativo de legislación de los delitos informáticos tipificados y penalizados en los países latinoamericanos escogidos frente a los sancionados en Colombia con el objeto de realizar un estudio en donde

se pueda identificar las falencias existentes en la normativa legal colombiana.

- ✓ Se analizará diversos artículos de investigación, estudios, ensayos y tesis que permitan tener claridad y determinación de la problemática y evolución de los delitos informáticos en Colombia.

- ✓ Se estudiará las diferentes sentencias de ley emitidas en cumplimiento de la Ley 1273 por los entes de control como la fiscalía y la corte suprema de justicia que permitan tener un conocimiento amplio del tema y a la vez hacer un análisis de las mismas en busca de las posibles ambigüedades y falencias de la ley en su acción de contrarrestar los problemas de seguridad informática en el país.

- ✓ Se realizará un análisis de fortalezas y debilidades de la legislación Colombiana que permita identificar sus dificultades, con el fin de formular una guía de propuestas en busca de la mejora de la misma, como parte de un instrumento legal más cercano a la realidad y la mitigación de la problemática planteada.

- ✓ Creación de una guía que evidencie propuestas puntuales que contribuyan a mejorar la legislación Colombiana contrarrestando la problemática de seguridad informática y de protección de datos actual.

7. LÍNEA DE TIEMPO SOBRE LA EVOLUCIÓN DE LOS DELITOS INFORMÁTICOS EN COLOMBIA

En Colombia no hay referencia sobre una fecha exacta del comienzo de los delitos informáticos, sin embargo los acontecimientos que acompañan cada delito o siniestro cometido contra la seguridad de la información en el territorio colombiano, permiten tener un lapso de tiempo de referencia que sirve de base para su estudio y análisis según sea el caso.

Por esta razón, se puede denotar que desde comienzos de los años 90's se sugiere el inicio de la cibercriminalidad, sin embargo en Colombia se tienen los primeros registros de esta actividad a partir del año 2002, más exactamente el 9 de Noviembre de ese año cuando la policía captura 17 personas que mediante el uso de técnicas de estafa y herramientas informáticas lograron la captación cerca de 160.000.000 millones de pesos, los cuales fueron transferidos a 350 cuentas bancarias. El delito logro llevarse a cabo mediante el uso de cuentas falsas y el acceso abusivo a los sistemas informáticos de las entidades financieras, dentro de los capturados había la figura de un "hacker" denominado alias "Repo" quien era el encargado de manipular el sistema de la entidad y de esta manera conseguir los privilegios de administrador para aprobar las transferencias a realizar desde las diferentes sucursales de la misma y de esta manera desviar los recursos hacia cuentas dispuestas para este trámite.

Por consiguiente, se observa uno de los primeros casos de acceso abusivo del cual se tiene documentación en el país y como al pasar el tiempo se hace más frecuente si se compara con la actualidad en donde es relativamente fácil que un individuo con conocimientos avanzados en el campo de la informática pueda llegar a materializar el robo de recursos de cuentas inactivas, pertenecientes tal vez aquellas personas que no mueven sus cuentas o que no se percatan del saldo que poseen. Este tipo de delito es muy común y afecta de manera considerable al detrimento patrimonial de una persona natural o de alguna empresa.

En los siguientes años al 2002, se propago con más fuerza los hurtos por medios informáticos gracias al crecimiento de la internet y de las diversas facilidades que

ofrece la red para realizar pagos, transferencias, compras, entre otras operaciones que en manos de personas incautas que no conozcan los protocolos y recomendaciones de seguridad en la red, pueden ser fácilmente victimas de los delincuentes informáticos que están siempre al asecho, mediante la creación de perfiles falsos, por ejemplo para captar la atención y conseguir datos importantes de la potencial victima, así como del uso de correos electrónicos con formularios idénticos por decirlo de alguna manera de las entidades ya sean bancarias o de otra índole en donde invitan a diligenciar contraseñas para acceder a promociones o rifas y por este medio conseguir el trofeo mayor, el hurto de información y económico que tanto desean.

Para el año 2007, se presenta el primer proyecto de ley de delitos informáticos por el señor Alexander Díaz, quien es el autor de dicha ley que fue impulsada por medio de los representantes de cámara German Varón Cotrino, Carlos Arturo Piedrahita y Luis Humberto Gallo. El objetivo principal de este proyecto de ley es crear un nuevo bien jurídico cuyo beneficio sea la protección de la información y el castigo contra nuevas formas de delincuencia que aparecieron junto con el uso de las nuevas tecnologías y que difieren con la tipificación legal existente de los delitos tradicionales que ampara el código penal colombiano y las diferentes leyes y decretos.

Siguiendo con la evolución de la delincuencia informática en Colombia, en el 2008 fue un año que estuvo caracterizado por el ataque mediante virus informáticos de forma masiva, un ejemplo destacado de esta actividad delictiva practicada por los “hackers” fue el llamado “Virus Medellín”, que al mejor estilo del famoso ataque con el virus “I Love you” del año 2000, también infectó gran parte de los computadores del departamento de Santander y se propagó mediante el uso de las memorias USB y correos electrónicos, este particular virus tenia la finalidad de infectar los equipos mediante la activación de un subject el cual destruía el arranque del equipo y lo dejaba inservible.

Con este ejemplo, se muestra la intencionalidad del daño informático que en este caso en particular busca el borrado de la información como tal y el daño en bien ajeno de los dispositivos, por el simple placer de ver comprometido todo un complejo de sistemas anidados a una red y tener así el control de la situación, tal

vez con el fin de darse a conocer como un individuo habilidoso en temas relacionados con el área de los sistemas, como lo hizo este delincuente informático en ese momento, en cuanto a que este daño no fue solamente un problema de unos cuantos computadores de un colegio, sino que fue de grandes ligas, puesto que afectó gran parte del departamento de Santander y a compañías prestigiosas a nivel regional, municipal como entes territoriales e inclusive sucursales de las diferentes compañías nacionales.

En 2009, es sancionada y entra en vigencia la ley 1273 de 2009 “De la protección de la información y de los datos” cuyo autor es el juez Alexander Díaz García, de esta manera se comienza el camino para la preservación de la información, los sistemas o dispositivos que utilicen las nuevas tecnologías y comunicaciones, entre otras disposiciones que reglamenta el nuevo bien jurídico anexado como un subtitulo dentro del código penal Colombiano, cuya finalidad es hacerle frente a partir de ese momento a la criminalidad en otro ámbito y ampliar el marco jurídico colombiano para la penalización de actividades delictivas que perjudiquen los bienes materiales y digitales de los colombianos.

No obstante, después de sancionada la ley que logró mitigar y judicializar a partir de su vigencia casos representativos a nivel nacional de los daños producidos por la materialización o comisión de delitos informáticos, estos han ido creciendo de forma alarmante en el país y cada vez son más avanzadas las técnicas empleadas por los ciberdelincuentes, a esto se suma que la herramienta jurídica presenta vacíos y ambigüedades que los jueces y fiscales al tomar una decisión jurídica no tienen claro como judicializar el delito, si de forma tradicional de acuerdo a la norma o con la tipificación realizada que se encuentra en la ley 1273 de 2009. Sin embargo para muchos estudiosos del tema profesionales en el área del derecho y la informática es de vital importancia tener claro como se deben tratar estos casos, puesto que una mala decisión perjudicaría a una persona o empresa y dejaría sin castigo o multa alguna al criminal.

Es así, que siguiendo con el estudio de los miles de casos que se cometen en Colombia se encuentra, que ya no solo es el robo de dinero por medios informáticos, sino que también se utiliza la ingeniería social para realizar ataques que llevan de un acceso no autorizado hasta la suplantación de identidad y la

denegación de servicios de un sistema por completo. Un ejemplo claro de este tipo de situaciones se puede observar en la comisión de delitos utilizando estos medios en los años 2010 al 2011, en donde lograron atacar y denegar servicios en la página de la registraduría nacional del estado civil, pasando por la web del senado y llegando inclusive a las páginas de algunos ministerios como el del interior y justicia. Es aquí donde se comienza a ver el “modus operandi” de los criminales que ya no atacan individualmente, sino que por el contrario forman sociedades de hackers como la famosa “Anonymus”.

Durante el periodo de 2012 hasta el año 2015, se presentó una variante en los casos de delitos informáticos, debido a que aumentaron de forma exponencial paralelo a las nuevas modalidades de delincuencia cibernética, dentro de estos se encuentran el cyberbullying, el acoso a menores a través de la red o el llamado “sexting” que esta en auge, en donde las personas que cometen este atentado contra la moral y violación a la intimidad son por lo general pedófilos o integrantes de redes de trata de personas que buscan captar la atención de menores de edad con el fin de ganar su confianza y hacer que los mismos accedan a deseos e instrucciones dadas por los criminales mediante el uso de la intimidación y el chantaje.

Por otro lado, el cyberbullying ha tomado fuerza en el último año y en lo corrido de 2016 se han conocido varios casos muy comentados en el país uno de ellos ocurrió a mediados del mes de Abril en donde un famoso youtuber llevó su gato a un veterinario, tiempo después el animal murió y éste culpó de la muerte del animal al médico veterinario y la clínica, por cuanto se ocupó de realizar una campaña agresiva por las redes sociales e incitando a sus seguidores que atentarán contra la vida del veterinario, sin embargo fue un caso sin resolver por parte de las autoridades, según investigación no se logró judicializar al youtuber por la conducta que sostuvo en las redes, debido a que el cybernullying no se encuentra tipificado dentro de la ley y no se tiene como referenciarlo dentro de la norma legal colombiana, por cuanto éste quedó en libertad.

7.1 ANÁLISIS DE LOS DELITOS INFORMÁTICOS FRENTE AL ACTUAL MARCO LEGISLATIVO INTERNACIONAL Y LA LEY 1273 COLOMBIANA

De acuerdo a la evolución de los delitos informáticos o ciberdelincuencia en Colombia, se puede observar que desde sus inicios hasta la actualidad han ido en constante crecimiento, aprovechando las diversas modalidades que da el uso de las TIC'S, teniendo en cuenta que el auge de las nuevas tecnologías son un medio de fácil acceso, así por ejemplo entre más personas estén conectadas a una red Wifi pública más fácil será que sus datos personales, contraseñas y demás archivos estén expuestos a ser robados por individuos que esperan la oportunidad.

Tomando como referencia, el informe que saca anualmente la compañía Symantec –Norton en 2015 aumentó en un 64% los ataques y amenazas informáticas, según ese estudio se recibieron más de 7.118 denuncias, que es una cifra bastante preocupante si se compara con el año inmediatamente anterior. Esta situación pone en tela de juicio los avances realizados con respecto al bien jurídico creado en 2009 para la protección de los datos y la información en Colombia y también la legislación internacional frente a esta problemática haciendo especial referencia al convenio de Budapest, el cual ha servido de base para la mayoría de países incluido Colombia para determinar unas normas o políticas frente a la seguridad informática y mitigar el daño causado a las personas del común y las empresas por medio de este flagelo.

Por esta razón, es importante tener en cuenta la actuación de la actual legislación, su estructura y componentes jurídicos frente a la evolución de los delitos cometidos a la información y de esta manera determinar, si realmente se esta cumpliendo con el objetivo real para lo cual fueron creadas estas leyes o si es necesario replantear su definición inicial y adicionar nuevas temáticas, clasificaciones y referencias legales que puedan alcanzar este objetivo, para que de esta manera se pueda tener un mayor control frente al flagelo creciente de seguridad en el mundo digital de la actualidad teniendo en cuenta, que la información no solo es digital sino que también se encuentra en medio físico y que ambas poseen un valor relevante para el funcionamiento no solo de una empresa y su medio de negocios, sino así mismo de una economía de un país entero.

Por lo expuesto anteriormente, a continuación se muestra un análisis detallado de la comisión de delitos informáticos en el país en los últimos años, con el fin de tomar una referencia más cercana a la actualidad que se vive frente a la problemática tratada. El cual permite analizar este flagelo con respecto al marco legislativo internacional y el nacional.

Tabla 1. Número de denuncias de delitos informáticos recibidas año 2013

Año	Delito	Número de denuncias recibidas	Porcentaje	Artículos infringidos Ley Colombiana	Artículos infringidos Convenio de Budapest
2013	Estafa	203	28.15%	Artículo 269I	Artículo 8
	Phishing	142	19.70%	Artículo 269G	Artículo 6
	Injuria y/o calumnia	74	10.26%	Artículo 221 C.P	No clasificado
	Skimming	73	10.12%	Artículo 269I, Artículo 269J	Artículo 3, Artículo 6
	Carta nigeriana	61	8.46%	Artículo 269I	Artículo 6, Artículo 8
	Suplantación de identidad	60	8.32%	Artículo 269F, Artículo 269G	Artículo 6
	Smishing	38	5.27%	Artículo 269G	Artículo 6
	Defacement	32	4.43%	No clasificado	No clasificado
	Sexting	25	3.46%	No clasificado	No clasificado
	Cyberbullying	13	1.83%	No clasificado	No clasificado
Total		721			

Fuente: El autor. Datos obtenidos de la página centro cibernético policial http://www.ccp.gov.co/ciberincidentes/tiempo-real/historico

Tabla 2. Número de denuncias de delitos informáticos recibidas año 2014

Año	Delito	Número de denuncias recibidas	Porcentaje	Artículos infringidos Ley Colombiana	Artículos infringidos Convenio de Budapest
2014	Estafa	1008	44,42%	Artículo 269I	Artículo 8
	Injuria y/o calumnia	267	11,77%	Artículo 221 C.P	
	Phishing	201	8,86%	Artículo 269G	Artículo 6
	Cyberbullying	186	8,2%	No clasificado	
	Carta nigeriana	152	6,7%	Artículo 269I	Artículo 6, Artículo 8
	Smishing	146	6,43%	Artículo 269G	Artículo 6
	Suplantación de identidad	100	4,41%	Artículo 269F, Artículo 269G	Artículo 6
	Sextorsión	91	4,01%	No clasificado	
	Vishing	71	3,13%	Artículo 269F, Artículo 269H	Artículo 6, Artículo 8
	Malware	48	2,12%	Artículo 269E	Artículo 4, Artículo 5
Total		2.269			

Fuente: El autor. Datos obtenidos de la página centro cibernético policial http://www.ccp.gov.co/ciberincidentes/tiempo-real/historico

Tabla 3. Número de denuncias de delitos informáticos recibidas año 2015

Año	Delito	Número de denuncias recibidas	Porcentaje	Artículos infringidos Ley Colombiana	Artículos infringidos Convenio de Budapest
2015	Hurto	4.572	64%	Artículo 269I	Artículo 6, Artículo 8
	Acceso abusivo a un sistema informático	1.087	15.27%	Artículo 269A	Artículo 2
	Violación de datos personales	965	13.5%	Artículo 269F	Artículo 10, 21, 3

Tabla 3. (Continuación)

Año	Delito	Número de denuncias recibidas	Porcentaje	Artículos infringidos Ley Colombiana	Artículos infringidos Convenio de Budapest
2015	Transferencia de activos	279	3.9%	Artículo 269J	No clasificado
	Suplantación	198	2.7%	Artículo 269G	Artículo 6
	Software malicioso	17	0.2%	Artículo 269E	Artículo 4, Artículo 5
Total		7.118			

Fuente: El autor. Datos obtenidos de la página centro cibernético policial http://www.ccp.gov.co/ciberincidentes/tiempo-real/historico

Tabla 4. Porcentaje comparativo años 2013 - 2015

Año	Porcentaje de aumento
2013	*
2014	68%
2015	64%

Fuente: El autor. Datos obtenidos de la página centro cibernético policial http://www.ccp.gov.co/ciberincidentes/tiempo-real/historico

(*) Nota: A partir de este año se inicia un proceso de estadística concreto que permite mantener un control sobre los indicadores del cibercrimen

8. COMPARATIVO DE LA LEY 1273 DE 2009 FRENTE A LAS LEYES CONTRA DELITOS INFORMÁTICOS DE ARGENTINA, CHILE Y VENEZUELA

Con el objetivo de establecer las diferencias y similitudes de la legislación colombiana contra los delitos informáticos a continuación se hace el comparativo frente a la legislación de Argentina, Chile y Venezuela, tomando como marco de referencia internacional los delitos establecidos y reconocidos en el Convenio de Budapest

Tabla 5. Comparativo legislativo

Delitos contemplados en la legislación internacional Convenio de Budapest	**Ley Colombiana 1273 de 2009**	**Ley Argentina 26.388**	**Ley Chilena 19223**	**Ley especial contra los delitos informáticos Venezuela**
Art. 2: Acceso ilícito	Artículo 269A: Acceso abusivo a un sistema informático	Artículo 153 bis: si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.	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 6. Acceso indebido Artículo 9. Acceso indebido o sabotaje a sistemas protegidos Artículo 10. Posesión de equipos o prestación de servicios de sabotaje

Tabla 5. (Continuación)

Delitos contemplados en la legislación internacional Convenio de Budapest	Ley Colombiana 1273 de 2009	Ley Argentina 26.388	Ley Chilena 19223	Ley especial contra los delitos informáticos Venezuela
Art. 5: Ataques a la integridad del sistema	Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación	Artículo 9: Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos Artículo 197: el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida	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. Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo	No existe ley en Venezuela contra los ataques al sistema

Tabla 5. (Continuación)

Delitos contemplados en la legislación internacional Convenio de Budapest	Ley Colombiana 1273 de 2009	Ley Argentina 26.388	Ley Chilena 19223	Ley especial contra los delitos informáticos Venezuela
Art. 3: Interceptación ilícita	Artículo 269C: Interceptación de datos informáticos	Artículo 153: el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.	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 21. Violación de la privacidad de las comunicaciones

Tabla 5. (Continuación)

Delitos contemplados en la legislación internacional Convenio de Budapest	Ley Colombiana 1273 de 2009	Ley Argentina 26.388	Ley Chilena 19223	Ley especial contra los delitos informáticos Venezuela
		Artículo 155: el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.		
Art. 4: Ataques a la integridad de los datos	Artículo 269D: Daño Informático	Articulo 10: En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños	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. Si como consecuencia de estas conductas se afectaren los datos contenidos	Artículo 7. Sabotaje o daño a sistemas Artículo 8. Favorecimiento culposo del sabotaje o daño

Tabla 5. (Continuación)

Delitos contemplados en la legislación internacional Convenio de Budapest	Ley Colombiana 1273 de 2009	Ley Argentina 26.388	Ley Chilena 19223	Ley especial contra los delitos informáticos Venezuela
		Artículo 255: el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público	en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo 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.	
Art. 10: Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines.	Artículo 269F: Violación de datos personales	Articulo 3: Violación de Secretos y de la Privacidad Artículo 157 bis: el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;	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	Artículo 11. Espionaje informático Artículo 20. Violación de la privacidad de la data o información de carácter Personal Artículo 22. Revelación indebida de data o información de carácter Personal

Tabla 5. (Continuación)

Delitos contemplados en la legislación internacional Convenio de Budapest	Ley Colombiana 1273 de 2009	Ley Argentina 26.388	Ley Chilena 19223	Ley especial contra los delitos informáticos Venezuela
		2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales	pena se aumentará en un grado	Artículo 25. Apropiación de propiedad intelectual
Art. 11: Tentativa y complicidad	Artículo 269H: Circunstancias de agravación punitiva	Artículo 184: 1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones; 2. Producir infección o contagio en aves u otros animales domésticos; 3. Emplear substancias venenosas o corrosivas; 4. Cometer el delito en despoblado y en banda; 5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en		Artículo 27. Agravantes Artículo 28. Agravante especial Artículo 29. Penas accesorias.

Tabla 5. (Continuación)

Delitos contemplados en la legislación internacional Convenio de Budapest	Ley Colombiana 1273 de 2009	Ley Argentina 26.388	Ley Chilena 19223	Ley especial contra los delitos informáticos Venezuela
		tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos; 6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.		
Art. 8: Fraude informático	Artículo 269I: Hurto por medios informáticos y semejantes	No se contempla en específico contra el fraude informático	No se contempla en específico contra el fraude informático	Artículo 13. Hurto Artículo 16. Manejo fraudulento de tarjetas inteligentes o instrumentos análogos Artículo 19. Posesión de equipo para falsificaciones

Tabla 5. (Continuación)

Delitos contemplados en la legislación internacional Convenio de Budapest	Ley Colombiana 1273 de 2009	Ley Argentina 26.388	Ley Chilena 19223	Ley especial contra los delitos informáticos Venezuela
Art. 6: Abuso de los dispositivos	Artículo 269J: Transferencia no consentida de activos	No se contempla en específico contra la transferencia no consentida de activos	No se contempla en específico contra la transferencia no consentida de activos	Artículo 15. Obtención indebida de bienes o servicios Artículo 17. Apropiación de tarjetas inteligentes o instrumentos análogos Artículo 18. Provisión indebida de bienes o servicios
Art. 9: Delitos informáticos relacionados con la pornografía infantil	Ley 679 de 2001 y ley 1339 de 2009	Artículo 128: el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare	No se contempla en específico este delito	Artículo 23. Difusión o exhibición de material pornográfico Artículo 24. Exhibición pornográfica de niños o adolescentes

Tabla 5. (Continuación)

Delitos contemplados en la legislación internacional Convenio de Budapest	Ley Colombiana 1273 de 2009	Ley Argentina 26.388	Ley Chilena 19223	Ley especial contra los delitos informáticos Venezuela
		espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.		
Art. 7: Falsificación informática	Artículo 269G: Suplantación de sitios web para capturar datos personales	No se contempla en específico este delito	No se contempla en específico este delito	Artículo 14. Fraude Artículo 26. Oferta engañosa Artículo 12. Falsificación de documentos.

Fuente: El autor. Legislaciones consultadas en las páginas propias de cada gobierno y asociación

8.1. DIFERENCIAS Y SIMILITUDES ENTRE LAS LEGISLACIONES

Dentro de la comparación efectuada en el cuadro anterior se puede observar que la ley colombiana 1273 de 2009 frente a las leyes internacionales tiene similitudes en la tipificación de algunos de los delitos informáticos, tal es el ejemplo del acceso abusivo o ilícito a sistemas informáticos en donde encaja perfectamente con la clasificación adoptada en el Convenio de Budapest y con las leyes que rigen actualmente en la temática de ciberdelincuencia en Venezuela, Argentina y Chile.

Sin embargo, las diferencias también son bastante notorias y es precisamente el objeto de estudio del presente proyecto, en donde mediante el análisis de las mismas se pueden adoptar medidas de corrección y adición a la normativa que actualmente rige el flagelo de la comisión de delitos por medio del uso de sistemas

informáticos o dispositivos que así lo permitan. A continuación se analizarán cada una de las diferencias:

8.1.1. ***Interceptación ilícita o de datos informáticos***. Este delito la ley colombiana lo clasifica dentro del artículo 269C, en donde hace referencia como su nombre lo indica a la interceptación de algún tipo de comunicación electrónica, sin embargo analizando este articulo frente a la ley Argentina en su artículo 153 y 155 de la ley 26.388, que lo considera desde todo punto de vista, es decir no solo habla de la interceptación como tal de un documento o mensaje electrónico, sino también de un documento o carta que sea apoderada por un tercero y que la divulgación o publicación de la información allí contenida es motivo de una sanción legal y económica.

La ley colombiana para este caso, se queda corta en el sentido que analizando el artículo 269C, solo habla de la interceptación en el origen, destino o en el interior de un sistema, a lo que le falta tener en cuenta la documentación de carácter físico que también es considerada importante dentro de la seguridad informática y que puede ser divulgada de igual manera utilizando un medio o dispositivo informático para causar daño a un tercero o en otros casos para obtener algún tipo de lucro.

Por otro lado, la ley 1273 de 2009 en su artículo 269C frente a la ley especial venezolana también difiere en el sentido que ésta trata la interceptación como violación a las comunicaciones y dentro de su artículo 21 hace referencia no solo a la interceptación sino también a la modificación, desvió o eliminación de la información que ha sido captura por medio del uso de tecnologías de información. Por consiguiente, hace falta dentro de la legislación colombiana ser más especifico en cuanto a denotar todas las formas de interceptación y manipulación de las comunicaciones, esto con el fin de tener mayor cobertura en el momento en el que se presente un hecho y que el mismo no se pueda clasificar del todo y de esta manera no permitir que por la existencia de este tipo de ambigüedad o vacío la comisión de un delito no se pueda juzgar y por lo tanto el delincuente quede en libertad o sin recibir alguna sanción económica como mínimo

8.1.2. *Fraude informático*. Teniendo en cuenta que el fraude como tal, es la acción de sacar provecho perjudicando a un tercero y de acuerdo al tratado internacional contra la ciberdelincuencia el Convenio de Budapest se concibe como el que atenta contra la información mediante el uso de herramientas tecnológicas para insertar instrucciones o código que permita la alteración, el borrado o daño de la información, se observa en comparación que en Colombia dentro de la ley 1273 de 2009 se podría ubicar en su artículo 269G el cual lo contempla 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"[72] al igual que en la ley especial venezolana quien lo toma de manera similar "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".

Se podría decir que ambas leyes son muy generales a la hora de clasificar este delito que es un de los más comunes en llevarse a cabo utilizando diversas técnicas, sin embargo hablando en especifico del articulo 269G de la ley colombiana solo se haría énfasis en el phishing o suplantación ya sea por medio de la falsificación de perfil, el entorno de una pagina web o el envío de un enlace, dejando de esta manera por fuera otras formas de cometer fraude como por ejemplo la "carta nigeriana" que es un correo electrónico en donde se pide el numero de cuenta de la victima para que le sea consignado un premio y de la misma forma se le pide que gire a una cuenta un abono por anticipado. Otro ejemplo son las llamadas telefónicas, mensajes vía Whatsapp o por interacción física (ingeniería social) utilizando algún dispositivo electrónico como tarjetas inteligentes donde se puede cometer fraude y en este caso no se podría clasificar dentro de la ley como tal, otorgando al delincuente un beneficio por la misma generalidad y/o ambigüedad en la que esta estructurada la ley.

En este orden de ideas, es necesario que la ley colombiana sea más especifica a la hora de clasificar este tipo de delitos por medios informáticos, con el fin de abarcar un rango más amplio y acomodándose de igual forma al avance tecnológico y a las necesidades de seguridad de la información, en donde se

[72] Ley 1273 de 2009 Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

permita tener un mayor control y prevenir ataques contra el patrimonio de los usuarios, de igual manera será mas fácil para los jueces y autoridades administrativas catalogar la comisión de delitos de fraude informático e imponer la pena sancionatoria correspondiente a lo que dicte el bien jurídico.

8.1.3. ***Delitos informáticos relacionados con la pornografía infantil***. En este caso Argentina y Venezuela tienen dentro de su marco legislativo contra la delincuencia informática un espacio para la temática de la pornografía infantil, no haciéndola ajena al tipo de conducta delictiva relacionada con los medios informáticos o como comúnmente se denomina uso de las TIC'S, caso contrario a lo que se puede observar en el ámbito jurídico colombiano que a pesar mencionar el delito de pornografía infantil en las leyes 1339 y 679 respectivamente, no se tiene en cuenta en específico la comisión de este delito por medios informáticos, se habla de manera general y solo se imponen sanciones administrativas.

Sin embargo, con el alarmante crecimiento de la comisión de delitos que abarcan este tema como el llamado "sexting" o "cibergrooming", en donde no solamente se pueden obtener imágenes de índole sexual de menores de edad sino que también puede llegar al punto de encuentros físicos por medio de la confianza generada entre el adulto que comete el delito y el menor. Por lo anterior, es importante tener en cuenta este tipo de actos delictivos caracterizándolos de manera más específica y no tan general en donde se da el espacio perfecto para el vacío legal o la ambigüedad que no permita su penalización en su momento por parte de la autoridad administrativa.

8.1.4. ***Ataques a la integridad del sistema***. En este apartado hace referencia aquellos delitos cometidos contra la integridad del sistema propiamente dicho, ya sea a su software o hardware por medio de la utilización de medios informáticos o dispositivos que permitan la materialización del delito. En el comparativo se puede observar que la ley colombiana lo tipifica en un artículo independiente mientras que las leyes de los países como Argentina, Venezuela y Chile hacen referencia a este tema dentro de los artículos que tratan sobre sabotaje informático respectivamente.

Sin embargo, la ley colombiana deja por fuera los casos en los cuales los funcionarios de empresas hacen caso omiso a las normas de seguridad en donde esta prohibido la instalación de software no autorizado, lo que representa la integridad del sistema como es el caso de los programas de descarga de música, juegos u otro tipo de aplicaciones que pueden dañar el sistema, debido a que al realizar la acción de descarga se pueden también bajar de esta manera virus que causen daño a la computadora y su correcto funcionamiento.

8.1.5. ***Falsificación de documentos digitales***. Para el caso de este delito se observa que la ley colombiana no tiene contemplada la falsificación de un documento electrónico como tal, puesto que solo consagra la falsedad de documento en los artículos 286-289[73] del vigente C.P. sin embargo, este delito puede cometerse en los casos en que el delincuente informático incluya un documento, altere, borre, etc. Por medio del uso de un dispositivo informático o cuando el documento repose en un equipo de computo o lo que haga sus veces como tablets, celulares, etc., realmente es una falencia puesto que en el actual código penal solo se consagra el delito de falsedad en documento público o privado en el caso de que el mismo sea físico y dentro de la ley 1273 no se encuentra estipulado como tal en ninguno de sus artículos o por lo menos, no de forma específica.

Esta situación no ocurre en la ley especial contra delitos informáticos venezolana en donde tiene bien estipulado esta conducta delictiva en su artículo 12, en donde sí hace referencia como "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"[74], lo que permite tener una figura más amplia para juzgar los delitos de este tipo cuando se presenten y no dar a lugar a dudas sobre cual ley aplicar de acuerdo al hecho cometido.

Por lo que se considera necesario, dentro de la legislación colombiana ser más específicos en este tipo de delitos informáticos, debido a que con el avance de las

[73] Ley 599 de 2000. Capítulo tercero De la falsedad en documentos Art. 286-289 Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

[74] Gaceta oficial de la república bolivariana de Venezuela. Ley especial contra los delitos informáticos. Art. 12 Disponible en http://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

nuevas tecnologías y el constante uso de firmas digitales, electrónicas y certificados es probable que pueda prestarse para cometer un ilícito en contra de la disponibilidad, integridad, confiabilidad y autenticidad de la información y pueda ser juzgada como falsedad que sería lo correcto y no como fraude.

9. ANÁLISIS SENTENCIAS DE LEY EMITIDAS EN CUMPLIMIENTO DE LA LEY 1273

Continuando con el estudio propuesto a la ley 1273 frente a los delitos informáticos cometidos en Colombia a continuación se realizará un análisis a las sentencias emitidas por la corte suprema de justica a partir de la vigencia de la presente ley, con el fin de seguir ahondando en la revisión de las posibles falencias y ambigüedades de la misma.

9.1. SENTENCIA SP1245-2015 DE FECHA 11 DE FEBRERO DE 2015

Esta sentencia emitida por la corte suprema de justicia sala de casación penal, cuyo objeto es "Establecer si el delito de hurto por medios informáticos y semejantes admite la figura de la reparación integral, descrita en el artículo 269 del Código Penal y, por ende, si los jueces de instancia incurrieron en la infracción directa de la ley sustancial por falta de aplicación de esa norma como consecuencia de la interpretación errónea del canon 269I ejusdem, al negar dicho derecho punitivo al procesado"[75]

Por ende, se realiza un estudio a profundidad de los artículos 269I y 269J correspondientes a hurto por medios informáticos y semejantes y la transferencia no consentida de activos, los cuales se crearon en la ley 1273 de 2009, con lo que se busca castigar la actividad delictiva que integra el uso de medios informáticos y afines. Dentro del documento se encuentra que analizando los dos bienes jurídicos, no era necesario su creación, puesto que preexisten normas a las cuales ejerciendo una amplia interpretación de los tipos penales de hurto calificado y estafa logran encajar perfectamente, cómo se puede consultar en el artículo 239 y siguientes del Código Penal colombiano.

Sin embrago, es necesario aclarar que en el caso de la transferencia no consentida de activos, si era notoria la necesidad de incluir un agravante que lograra traer consigo la figura jurídica, en donde se demuestre este

[75] Sentencia SP1245-2015 Disponible en http://190.24.134.101/corte/wp-content/uploads/relatorias/pe/b1mar2015/SP1245-2015.pdf

comportamiento delictivo haciendo uso de los medios informáticos y teniendo presente que lo que dentro de este bien surge es el tipo de estafa sin contacto con la víctima, debido a que se utilizan redes. Al mismo tiempo, se tiene en cuenta que al cometer dicha acción o comportamiento se infringen los artículos 269A – 269F de la presente ley 1273 y no solo los dos artículos 269I y 269J.

Por otro lado, se menciona la reparación integral en donde como bien se sabe es un derecho no un beneficio, el cual está consagrado en el artículo 269 del Código Penal que consiste en la reducción de la mitad a las tres cuartas partes de la pena en favor del condenado, cuando el mismo hubiese restituido el bien mueble o valor económico correspondiente del delito a la víctima o perjudicado antes de realizarse el fallo en primera instancia. Esto da a entender, que en la mayoría de los casos que se presente con delitos los cuales tengan el tipo penal de hurto o estafa por medios informáticos si el acusado devuelve el valor del hurto cometido quedaría con una rebaja de pena, dejándolo en libertad en muy poco tiempo y al mismo tiempo deja en entre dicho la severidad de las sanciones las cuales están consagradas en la ley 1273 que busca la protección de los datos e información y que se creó precisamente con sanciones con el máximo castigo, por decirlo así con el fin de contrarrestar el volumen de delitos de este tipo.

Esta ponencia de la presente sentencia, también demuestra la ambigüedad de la ley en cuanto a que en la interpretación de los jueces o autoridades pertinentes que revisen y juzguen este tipo de delitos los lleguen a considerar dentro de la figura jurídica de hurto calificado, por lo tanto no entraría a revisarse como delito por hurto por medios informáticos y semejantes, así mismo como transferencia de activos lo que deja al bien jurídico creado sin efecto alguno.

Por lo cual, se genera una pregunta de rigor como es ¿En realidad fue necesario crear estos dos artículos? y ¿Por qué no deroga artículos anteriores del Código Penal, para no crear confusiones a las autoridades competentes?

9.2. SENTENCIA 34564 DEFINICIÓN DE COMPETENCIA DE 25 DE AGOSTO DE 2010.

Cuyo objeto de investigación se faculto en los hechos cometidos que se describen a continuación:

> *"Del escrito de acusación se puede extractar que por medio de una transacción bancaria realizada el 28 de mayo de 2009, originada desde la ciudad de Barranquilla, de manera ilícita y superando barreras electrónicas, se trasfirió a varios destinos bancarios (nueve cuentas) la suma de ciento nueve millones de pesos ($ 109.000.000.oo) que estaban en una cuenta de Bancolombia, de la Oficina ubicada en el Centro Comercial Campanario de la ciudad de Popayán, de propiedad del mismo Centro Comercial."*[76]

En este caso, una vez analizado se encuentra que existe falencia en cuanto a la competencia de juzgamiento de los delitos cometidos por hurto por medios informáticos y semejantes, debido a que como se evidencia en el presente caso la ciudad donde se realizó la manipulación de la información y la transferencia de activos fue Barranquilla, sin embargo el delito se consumó en las cuentas cuya procedencia está situada en la entidad bancaria de la ciudad de Popayán.

Por consiguiente, se realizó la denuncia en el juzgado octavo penal del circuito de Barranquilla, en donde el juez asignado determinó que no era de su competencia territorial y por lo tanto remitió el proceso al juzgado penal municipal con funciones de conocimiento de la ciudad de Popayán, a lo que el mismo da como respuesta que a pesar que el hecho delictivo se consumó en esa ciudad, no fue donde se originó el mismo.

Por lo tanto, el proceso llegó a la sala de casación penal de la corte suprema de justicia para que la misma determinara la competencia de la autoridad correspondiente para realizar el juzgamiento del hecho delictivo. Esta resuelve que de acuerdo al artículo 37 del Código de Procedimiento Penal, la cual asigna a los

[76] Sentencia 34564 Disponible en http://es.slideshare.net/Alediaganet/sentencia-34564-25-08-10-competencia-transferencia-activos

jueces penales municipales la competencia para el conocimiento de los delitos contenidos en el Título VII Bis del Código Penal, el cual corresponde expresamente a la Ley 1273 de 2009, declarar que la competencia para adelantar dicho juzgamiento correspondiente a las actuaciones procesales es el juzgado penal municipal con funciones de conocimiento de la ciudad de Popayán.

De esta forma, se puede observar la falencia en cuanto a la tipificación del delito como primera instancia, debido a que lo juzgaron como hurto calificado, siendo lo correcto lo descrito en el artículo 269I “Hurto por medios informáticos y semejantes” y sin embargo es una clara infracción del artículo 269J “Transferencia no consentida de activos”, estas dos situaciones sumada a la falta de capacitación sobre la competencia de las autoridades judiciales para el conocimiento y juzgamiento del delito hace que primero se demore más tiempo las actuaciones pertinentes y segundo crea la duda si realmente se está juzgando el delito de forma correcta de acuerdo a la norma correspondiente.

Al igual que en el análisis de la primera sentencia se observa no solo las falencias, sino también ambigüedades de la misma ley , lo que no permite un correcto funcionamiento de la misma, dejando de esta manera que en muchos casos se puedan vencer términos en cuanto definen la competencia de la autoridad y de esta manera quedarían muchos delitos informáticos sin el debido castigo, al igual que sus infractores en plena libertad para seguir cometiendo este tipo de hechos a sabiendas que pueden burlar la ley.

9.3. AMBIGUEDADES Y/O FALENCIAS DE LA LEY 1273 DE 2009

Dentro del análisis a la ley 1273 se encuentra que dentro de su estructura jurídica deja varias ambigüedades, las cuales en su momento podrían ser una dificultad al penalizar los diferentes delitos informáticos cometidos en Colombia, por lo que es necesario analizar estas posibles falencias en busca de un modelo correctivo que pueda mejorar la legislación y mitigar los daños causados y prevenir a futuro mediante su conocimiento y socialización la comisión de delitos por medios informáticos.

Por consiguiente, realizando un análisis se encuentra que dentro del artículo 269C el cual trata sobre la 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”, aquí la ley es bastante general buscando abarcar todos los ámbitos en donde se puede presentar la interceptación de la información, pero que pasa si una persona utiliza herramientas para el escaneo de puertos o test de vulnerabilidad a un sistema de forma empírica y no se apodera de ninguna información? Es una interrogante que sale a flote ya que revisando el artículo no se podría catalogar como delito, debido a que no se esta alterando o capturando como tal la información a pesar de realizar una acción que puede vulnerar el sistema por decirlo de algún modo, este tipo de conducta requiere que la ley sea más específica puesto que es muy fácil traspasar la delgada línea entre lo licito y lo ilícito y se podría incurrir en la penalización de un individuo injustamente o por el contrario dejar sin castigo a quien lo merezca.

Otra falencia de la presente ley esta reflejada en el artículo 269G “Suplantación de sitios web para capturar datos personales. 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”, en esta parte se deja a interpretación por ejemplo si casos como el spam puede considerarse como delito informático, esto pensado como a través de este medio se puede filtrar muchas veces correos que no propiamente son basura y que por el contrario son enviados con el fin de apoderarse de algún tipo de información confidencial de la víctima y de esta manera atentar contra la privacidad e incurrir en otro delito aún más grande llegando a la estafa, falsificación, entre otros. De igual manera el spam puede llegar a saturar de tal manera un sistema de correo electrónico al punto de hacerlo colapsar, siendo este un motivo también de obstaculización del funcionamiento correcto del sistema por lo que se estaría infringiendo a su vez el artículo 269B.

Por otro lado, se observa que en el artículo 269E sobre el uso de software malicioso se considera como “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”, aquí hace falta clasificar adecuadamente que se considera software malicioso, puesto que solo encajaría los denominados virus, malware, troyanos,

gusanos, entre otros, pero que pasa con aquellas aplicaciones que son software defectuoso las cuales contienen bugs que podrían ser peligrosos para el sistema pero que no son intencionales y que si se revisan estadísticas en las empresas una de las causales de perdida de información o daño al sistema ocurre cuando un empleado sin intención aparente descarga e instala software que es “confiable” con diversos fines como descarga de música, juegos, etc. En este caso no se podría denominar delito de acuerdo al presente artículo y sin embargo se incurre en una acción que deja daños.

A pesar que la ley colombiana tiene similitudes con las leyes con las cuales fue comparada en la tabla 5, es importante señalar que en el caso del acceso abusivo aún hace falta clasificar dentro del artículo 269A el manejo de los dispositivos o herramientas informáticas, debido a que la ley en el fondo no es clara ya que solo habla del acceso como tal y no cuando se utilice un medio para conseguirlo, como si se toma en cuenta en la ley especial venezolana en su artículo 10 en donde hace un especial énfasis en esta situación, con el fin de no dejar espacios vulnerables dentro de la misma y de esta manera aclarar el tema para poder ejecutar con determinación y claridad absoluta el castigo correspondiente cuando se viole la ley.

Siguiendo con el análisis requerido a los artículos de la ley 1273 y revisando las sentencias emitidas sobre los apartados 269I “Hurto por medios informáticos y semejantes” y 269J “Transferencias no consentida de activos”, se observa la ambigüedad y falencia existente dentro de lo consagrado a la presente ley con respecto a la protección de la información y los activos ya sean de carácter mueble o digital. En este caso las dos sentencias SP1245-2015 y 34564 permiten observar dos problemas notorios a la hora de poder realizar el debido juzgamiento a los delitos de hurto informático y transferencia de activos, puesto que revisando y como se mencionó en el análisis de las sentencias existen primero que todo normas ya vigentes que pueden castigar estas conductas punibles de acuerdo a la interpretación que se les haga y en segunda instancia no es claro quien es la autoridad competente para llevar el caso, debido a la interpretación que se da en cuanto a donde se origina y donde se consuma el delito como tal.

Este tipo de situaciones hacen difícil el proceder legal y también permiten generar dudas sobre la capacidad legislativa para brindar la protección necesaria en

cuanto a información y activos tangibles e intangibles se refiere, por cuanto sería recomendable definir con claridad las conductas punibles que se consideren para el caso del hurto por medios informáticos y si es necesario un apartado sobre éste o si por el contrario es conveniente adicionar un parágrafo o inciso agravante al artículo 240 del C.P. en cuanto a la transferencia de activos es la misma situación, debido a que es una técnica de estafa valiéndose del acceso abusivo y finalizando con la figura de hurto calificado, lo que debería especificarse o detallar aún más con el fin de no crear confusiones y por consiguiente dejar a diversas interpretaciones la situación.

Si bien es cierto que los delitos informáticos así como sus términos cambian al pasar el tiempo, es necesario que de igual manera el bien jurídico que se creó para brindar seguridad y tranquilidad en el manejo de la información por medios electrónicos y telemáticos debe ser acorde e ir un paso más adelante de las necesidades previstas hasta el momento y no dejar a interpretaciones superfluas acciones que coloquen en potencial riesgo la integridad, disponibilidad y confidencialidad de la información según sea su clasificación en el ámbito en el que se utilice.

Por esta razón, es necesario incluir dentro de este bien jurídico un apartado de las definiciones y aclaraciones concernientes a los diferentes delitos informáticos y los medios utilizados para su materialización o comisión, puesto que esto facilitaría la protección de la información y la correcta clasificación de los mismos dentro de la estructura legislativa, con el fin de dar el tratamiento adecuado según se amerite el caso.

10. PROPUESTAS QUE CONTRIBUYEN A MEJORAR LA LEGISLACIÓN COLOMBIANA CONTRARRESTANDO LA PROBLEMÁTICA DE SEGURIDAD INFORMÁTICA Y DE PROTECCIÓN DE DATOS ACTUAL

Después de analizar cada uno de los artículos de la ley 1273 de 2009, encontrar sus posibles falencias y/o ambigüedades y compararlos con cada una de las legislaciones vigentes en los países escogidos para ello, se pretende dar una posible solución a la problemática creciente de delitos informáticos en Colombia mediante una estrategia de propuestas puntuales dentro de esta ley, que permita favorecer a todas aquellas personas que se ven afectadas día a día con este flagelo y dar claridad dentro de la misma a jueces y fiscales con el fin que puedan definir dada la situación si merece la tipificación y castigo como delito informático o no a los casos que se denuncian a diario.

A continuación se muestra esta estrategia dividida en dos puntos principales, el primero formando un nuevo artículo de términos que puedan definir cada delito informático y que dicho artículo pueda considerarse como base de consulta jurídica e informática, en donde se pueda definir con claridad cada delito que utilice medios informáticos. El segundo punto se trata de redefinir cada artículo de la ley 1273 que contenga falencias analizadas en el desarrollo de este proyecto.

10.1. DEFINICIONES DELITOS INFORMÁTICOS

Dentro de la ley 1273 de 2009 denominada “de la protección de la información y de los datos”, añadida al Título VII Bis del código penal colombiano, se encuentra 10 artículos que la componen dividida en 2 capítulos, los cuales contemplan las acciones punitivas cometidas a través de delitos cometidos mediante uso de medios o sistemas informáticos.

10.1.1. Artículo de terminología de delitos informáticos. Los siguientes términos pertenecen al ámbito de la delincuencia informática actual:

Acceso no autorizado a servicios y sistemas informáticos: Son todas aquellas técnicas que pueden ir desde la simple curiosidad de un hacker principiante, con el fin de conocer y acceder sin permiso alguno a un sistema o red, hasta el sabotaje, robo, daño o espionaje de carácter informático llevado a cabo a través de técnicas y herramientas que facilitan el proceso con intencionalidad de obstaculizar el funcionamiento normal del sistema.

Bomba lógica: Son aplicaciones que van incrustadas dentro de otro código, cuyo objetivo principal es realizar un ataque de tipo malicioso contra un sistema principalmente dañando la parte lógica, es decir el funcionamiento de aplicaciones, borrando archivos o ficheros, inhabilitando el sistema operativo entre otras acciones.

Este tipo de ataque se diferencia del software malicioso, debido a su modo de operar, puesto que un software malicioso entra al sistema y se ejecuta casi de inmediato realizando el daño, mientras las bombas lógicas son capaces de quedar suspendidas o inactivas hasta que se cumpla un determinado tiempo que ha sido programado por el hacker o delincuente informático, en cuanto se cumpla el plazo que se haya estipulado la bomba se activa desarrollando las tareas para la cual fue programada.

Bot y Botnes: Se trata de un ataque por medio de software malicioso "bot" que convierte a una red de equipos infectados en "zombis" o "botnes", es decir que a través de este tipo de software malicioso el cual permanece oculto en la máquina infectada espera instrucciones del ciberdelincuente para comenzar el ataque.

A continuación se presenta una tabla con las tareas automatizadas que puede realizar un bot:

Tabla 6. Tareas de un bot

Enviar	**Robar**	**DoS** (denegación de servicio)	**Fraude mediante clic**
Envían -spam -virus -software espía	Roban información privada y personal y se la comunican al usuario malicioso: - números de tarjeta de crédito - credenciales bancarias - otra información personal	Lanzan ataques de denegación de servicio (DoS) contra un objetivo específico. Los criminales cibernéticos extorsionan a los propietarios de los sitios web por dinero, a cambio de devolverles el control de los sitios afectados.	Los estafadores utilizan bots para aumentar la facturación de la publicidad web al hacer clic en la publicidad de Internet de

Tabla 6. (Continuación)

Enviar	**Robar**	**DoS** (denegación de servicio)	**Fraude mediante clic**
	y confidencial	Sin embargo, los sistemas de los usuarios diarios son el objetivo más frecuente de estos ataques, que sólo buscan molestar.	manera automática.

Fuente: https://es.norton.com/botnet. Bots y botnets: una amenaza creciente

Carding: Es una forma de transferencia de activos que solo incluye a las tarjetas de crédito dentro de la comisión del ilícito como tal, se trata de utilizar de forma ilegal los números de las tarjetas de crédito para realizar la transferencia de activos directamente de la tarjeta de al victima a una cuenta o para realizar múltiples transacciones como compras.

Ciberacoso: Son todas aquellas amenazas, humillaciones, hostigamiento, entre otras manifestaciones que son llevadas a cabo por medio del uso de las nuevas tecnologías, como pueden ser correos electrónicos, mensajes de texto y whatsapp, publicaciones en redes sociales.

Ciber Bulliying: Consiste en la intimidación y agresión utilizando los diferentes medios informáticos entrando en un tipo de atentado contra la moral y la integridad de la persona. Sin embargo para que se pueda establecer que se trata de ciberbullying debe existir dos menores en ambos extremos de este ataque, ya que si de uno de los dos lados existe un adulto se convierte en otro tipo de acoso.

Child grooming: Es una forma de "captación" de menores para utilizarlos en espectáculos exhibicionistas de carácter sexual o bien para ser utilizados en la elaboración de material tipo pornográfico que es utilizado para distribución o beneficio propio. Esta técnica ttiene varias fases en las cuales el acosador a través de internet busca la confianza del menor, para que luego éste utilice la web cam como medio de comunicación y pueda acceder a lo que demanda el acosador con temas literalmente sexuales.

Data leakage (filtración de datos): Es una de las categorías del espionaje, la cual se conoce comúnmente como divulgación no autorizada de información o datos que son reservados. Esta técnica es utilizada por los delincuentes

informáticos cuando acceden sin autorización al sistema de una empresa, cuyo objetivo principal es sustraer información confidencial de la misma.

DDoS (Distributed Denial of Service): Es un ataque que consiste en un ataque masivo por así decirlo a un solo ordenador por parte de un grupo de sistemas comprometidos o grupo de equipos zombie que realizan su ataque a un único objetivo en donde dejan sin servicio al mismo. La idea de este ataque es enviar demasiadas peticiones al objetivo para que éste se sature, es decir, se quede sin recursos y deje de funcionar posteriormente.

De este tipo de ataque se conoce técnicas como slow read, la cual se constituye en el envío de tráfico muy lentamente lo que hace que colapse el número de sesiones disponibles del objetivo, otras técnica consiste en la alteración de los paquetes con el fin que el servidor se quede esperando de manera indefinida una respuesta de una dirección IP falsa.

Eavesdropping: Se conoce como la interceptación pasiva de un sistema o tráfico de red, es un ataque sin modificación de información, lo que busca es monitorear el tráfico de paquetes enviados o direccionados hacia una computadora a través de herramientas o aplicaciones tipo sniffer los cuales realizan todo el trabajo y son instalados propiamente en el equipo por un usuario con acceso de forma legítima o por un intruso que ha utilizado otra técnica para realizar su instalación. Esta forma de ataque es muy utilizada para sustraer los loginIDS y contraseñas de los usuarios en sistemas que son vulnerables y que de acuerdo al escaneo realizado se ha podido explotar alguna de sus vulnerabilidades que dejan al descubierto la información.

Keylogger: Es un programa que registra y graba la pulsación de teclas (y algunos también clicks del mouse). La información recolectada será utilizada luego por la persona que lo haya instalado. Actualmente existen dispositivos de hardware o bien aplicaciones (software) que realizan estas tareas. [77]

[77] Segu.Info seguridad de la información. Keylogger Disponible en http://www.segu-info.com.ar/malware/keylogger.htm

Los keyloggers pueden se físicos o por software, los primeros son instalados entre el computador y el teclado, estos dispositivos son pequeños y son imperceptibles para los usuarios inexpertos y los segundos son utilizados en diversos casos para controlar las acciones de forma remota como por ejemplo algunas empresas lo utilizan para controlar a los funcionarios y sus actividades, sin embargo puede ser catalogado como violación a la privacidad.

Malware: Son programas informáticos diseñados para realizar diversas acciones dañinas como tomar el control de un equipo, manejar remotamente algunas aplicaciones de la parte lógica (software) o robo de información. La clasificación de estos programas depende básicamente de las acciones que realicen sobre el sistema y de esta manera se pueden clasificar en virus, troyanos y gusanos. A continuación se define cada uno de estos términos:

- Virus: Inserta parte de su código interno dentro de programas legítimos. De este modo, un usuario podría estar ejecutando un software genuino y a la vez el virus si dicho archivo está infectado. [78]

- Gusano: Es código malicioso diseñado para propagarse automáticamente a través de cualquier medio como dispositivos de almacenamiento USB, discos duros, redes corporativas, redes sociales, etc. [79]

- Troyano: Es código malicioso que no se propaga automáticamente ni tampoco infecta archivos. La particularidad de los troyanos es que simulan ser programas legítimos y de utilidad, sin embargo, su objetivo es completamente contrario.[80]

Perfiles falsos: Se trata de 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.

[78] Semana (2014). ¿Qué es un Malware y cómo se puede prevenir? Disponible en http://www.semana.com/tecnologia/tips/articulo/que-malware-como-puede-prevenir/372913-3

[79] Semana (2014). ¿Qué es un Malware y cómo se puede prevenir? Disponible en http://www.semana.com/tecnologia/tips/articulo/que-malware-como-puede-prevenir/372913-3

[80] Semana (2014). ¿Qué es un Malware y cómo se puede prevenir? Disponible en http://www.semana.com/tecnologia/tips/articulo/que-malware-como-puede-prevenir/372913-3

Pornografía infantil: Se trata del uso de medios como redes sociales en donde abundan 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.

Pharming: Es una modalidad de ataque utilizada por los atacantes, que consiste en suplantar al Sistema de Resolución de Nombres de Dominio (DNS, Domain Name System) con el propósito de conducir a una página Web falsa. El atacante logra hacer esto al alterar el proceso de traducción entre la URL de una página y su dirección IP.

Para llevar a cabo redireccionamiento a las páginas Web falsas o maliciosas se requiere que el atacante logre instalar en el sistema alguna aplicación o programa malicioso (por ejemplo, un archivo ejecutable .exe, .zip, .rar, .doc, etc.). La entrada del código malicioso en el sistema puede producirse a través de distintos métodos, siendo la más común a través de un correo electrónico, aunque puede realizarse también a través de descargas por Internet o a través de unidades de almacenamiento removibles como una memoria USB.[81]

Ransomware: Es un tipo de software malicioso, que utiliza el ciberdelincuente con el fin de bloquear el acceso normal al equipo o computador, cifrar los archivos que se encuentren en el mismo y luego pedir un rescate para recobrar tanto el acceso al equipo como a la totalidad de archivos que han sido de alguna manera interceptados. Sin embargo durante este ataque no hay ninguna garantía que el delincuente cumpla con lo que promete en cuanto tenga el pago del rescate por cuanto se esta sujeto a perder información total o parcial.

Rounding down o técnica del salami: Es una modalidad de fraude por medios electrónicos, la cual consiste en transferir pequeñas cantidades de dinero de cuentas bancarias a través de unas instrucciones de repetición automáticas programadas previamente. Esta técnica es difícil de detectar y es realizada con facilidad por delincuente informático, un ejemplo es la modalidad llamada redondeo hacia abajo en donde se transfiere los centavos que se descuenten por el redondeo de las cuentas a una cuenta específica.

[81] Universidad Nacional Autónoma de México (2009). Eduteca. Manual para identificar y notificar phishing scam. Pharming Disponible en http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=194

Scavenging: Es una técnica conocida por apropiarse o recoger información residual la cual es abandonada o dejada sin protección alguna, en donde la misma puede encontrarse de forma física en las papeleras de basura o de forma electrónica, cuando la información es tomada de los medios magnéticos como memorias extraíbles (USB), CD, DVD o cualquier otro soporte de este tipo que este sin la debida protección.

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.

Scam o Phishing Laboral: Fraude similar al phishing, con el que comparte el objetivo de obtener datos confidenciales de usuarios, para acceder a sus cuentas bancarias. Consiste en el envío masivo de correos electrónicos o la publicación de anuncios en webs, en los que se ofrecen supuestos empleos muy bien remunerados. Cuando el usuario acepta la oferta de trabajo, se le solicita que facilite datos de sus cuentas bancarias, a través de un e-mail o accediendo a una web, para ingresarle los supuestos beneficios.[82]

Sniffing: Es la técnica de escaneo o escucha de redes mediante una aplicación informática (sniffer) que permite capturar, interpretar y almacenar los paquetes enviados a un ordenador mientras viajan por la red, dependiendo de la topología de la misma, debido a que ciertas topologías de red son más fáciles de interceptar y están conectadas al nodo central en donde se encuentra la información.

SMiShing: Es una variante del phishing, que utiliza los mensajes a teléfonos móviles, en lugar de los correos electrónicos, para realizar el ataque. El resto del procedimiento es igual al del phishing: el estafador suplanta la identidad de una entidad de confianza para solicitar al usuario que facilite sus datos, a través de otro SMS o accediendo a una página web falseada, idéntica a la de la entidad en cuestión.[83]

[82] Computer Forensic Recovery Labs (2015). Delitos informáticos. Glosario Disponible en http://www.delitosinformaticos.info/delitos_informaticos/glosario.html

[83] Computer Forensic Recovery Labs (2015). Delitos informáticos. Glosario Disponible en http://www.delitosinformaticos.info/delitos_informaticos/glosario.html

Spam: Consiste en el envío masivo de mensajes no solicitados, con contenido generalmente publicitario, que se realiza a través de distintos medios como: foros, mensajería instantánea, blogs, etc. aunque el sistema más utilizado es el correo electrónico. Para obtener la lista de direcciones de correo, los spammers o remitentes de "mensajes basura", emplean software especializado o robots que rastrean páginas web en busca de direcciones, compran bases de datos, utilizan programas de generación aleatoria de direcciones, copian las direcciones de listas de correo, etc.[84]

Spoofing: En términos de seguridad de redes hace referencia al uso de técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación, es decir, un atacante falsea el origen de los paquetes haciendo que la víctima piense que estos son de un host de confianza o autorizado para evitar la víctima lo detecte. En el spoofing entran en juego tres máquinas o hosts: un atacante, un atacado, y un sistema suplantado que tiene cierta relación con el atacado; para que el atacante pueda conseguir su objetivo necesita por un lado establecer una comunicación falseada con su objetivo, y por otro evitar que el equipo suplantado interfiera en el ataque.[85]

Spyware: Se trata de un software cuya finalidad es recopilar la información obtenida de un computador u ordenador (contactos, mensajes, correos electrónicos, etc.) para luego trasmitirla a una fuente externa sin el conocimiento previo del propietario del ordenador víctima, este ataque es conocido como una de las variantes de malware frecuentemente utilizado para el espionaje industrial.

Trashing: Es una técnica que consiste en el restreo o búsqueda en las papeleras de basura de las oficinas o sitios escogidos por el delincuente informático, en donde puede encontrar información valiosa que contenga por ejemplo números de cédula, tarjetas de crédito, teléfonos, entre otros datos que han sido arrojados sin las medidas de seguridad a la papelera.

[84] Computer Forensic Recovery Labs (2015). Delitos informáticos. Glosario Disponible en http://www.delitosinformaticos.info/delitos_informaticos/glosario.html

[85] García, C. (2010). Hacking ético. Hablemos de Spoofing Disponible en https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/

10.2. *ARTÍCULOS DE LA LEY 1273 MODIFICADOS*

Dentro del desarrollo del presente proyecto sobre la ley 1273 “de la protección de la información y de los datos”, frente a la evolución de los delitos informáticos en Colombia, se encuentra que después del análisis respectivo se da lugar a realizarse una modificación a algunos artículos de la presente ley con el fin de abarcar todos los campos de la comisión de delitos informáticos en el país, esto con el fin de presentar una mejora no solo en el ámbito jurídico sino también el área de seguridad informática y realzar la confianza de la ciudadanía sobre las figuras legales existentes que castiguen concretamente aquellos delitos que se presentan específicamente con el tema del uso de la informática en los diferentes campos de acción social, económico, administrativo, entre otros.

Por consiguiente, a continuación se presenta una mejora aquellos artículos que durante este estudio se encontraron falencias y/o ambigüedades, ya analizadas en apartados anteriores del presente documento:

10.2.1. ***Artículo 269A: Acceso abusivo a un sistema informático***. El que, sin autorización o por fuera de lo acordado, utilice equipos, dispositivos o programas para acceder 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.

Modificación: Se requiere definir dentro de este artículo el uso de dispositivos o programas para ejecutar el acceso abusivo a un sistema informático, para lo que se añade “El que, sin autorización o por fuera de lo acordado, utilice equipos, dispositivos o programas…” en donde se deja claro que quien utilice estos medios y no solo ejecute el hecho de acceder de forma abusiva a un sistema también reciba castigo al emplear o poseer dispositivos o herramientas que así lo permitan.

10.2.2. ***Artículo 269C: Interceptación de datos informáticos***. El que posea, adquiera o utilice con previo conocimiento o de formas empírica dispositivos o herramientas de tipo informático o telemático y sin orden judicial previa intercepte datos informáticos o documentos físicos 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.

Modificación: En este artículo se añade “El que posea, adquiera o utilice con previo conocimiento o de formas empírica dispositivos o herramientas de tipo informático o telemático y sin orden judicial previa intercepte datos informáticos o documentos físicos…”, esto con el fin de ser más específica la tipificación del delito de la interceptación de información y vincular el uso de dispositivos que puedan ser utilizados para cometer esta clase de delito, además de incluir los documentos o información de carácter físico que también hace parte del principio de salvaguarda de la seguridad informática.

10.2.3. ***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 o realice la instalación sin autorización de software o programas informáticos de no contengan licencia, 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.

Modificación: Se adiciona a este artículo “…realice la instalación sin autorización de software o programas informáticos de no contengan licencia…” lo que permite tener en cuenta el software que no se encuentra licenciado y que sin autorización puede llegar a descargarse e instalarse en los equipos de computo y que contengan sectores defectuosos (bugs) o virus que afecten la parte lógica y física de los sistemas de información.

10.2.4. ***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 entendiéndose para ello como virus, malware, troyanos, spyware o spam u otros programas de computación de efectos dañinos como aquellos que no contengan licencia para su instalación y puedan contener defectos (bugs) que causen daño a los dispositivos informáticos o telemáticos, 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

Modificación: Dentro de este artículo se incluye una definición más amplia de lo que significa software malicioso y programas de efecto dañino "…software malicioso entendiéndose para ello como virus, malware, troyanos, spyware o spam u otros programas de computación de efectos dañinos como aquellos que no contengan licencia para su instalación y puedan contener defectos (bugs) que causen daño a los dispositivos informáticos o telemáticos…", con la finalidad de clasificar mejor los mismos y poderles dar el tratamiento adecuado según sea el caso.

10.2.5. ***Artículo 269G: Suplantación para capturar datos personales***. El que con objeto ilícito y sin estar facultado para ello, suplante perfiles o cree perfiles falsos tanto en sitios web como en el manejo de las redes sociales, o realice suplantación de identidad mediante el uso de medios de comunicación telefónica y telemática y que a su vez diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, 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, siempre que la conducta no constituya delito sancionado con pena más grave.

Modificación: Se modifica el título del artículo a "Suplantación para capturar datos personales" y se añade la siguiente especificación "El que con objeto ilícito y sin estar facultado para ello, suplante perfiles o cree perfiles falsos tanto en sitios web como en el manejo de las redes sociales, o realice suplantación de identidad mediante el uso de medios de comunicación telefónica y telemática y que a su vez…", con el fin de vincular y regularizar la suplantación no solamente como el envió de enlaces propiamente sino también abarcando todo el ámbito en el cual se pueda generar una suplantación ya sea vía telefónica, mensajes de texto, whatsapp, el uso de perfiles falsos en redes sociales o sitios web de igual manera.

10.2.6. ***Artículo 269I: Hurto por medios informáticos y semejantes***. 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, incurrirá en las penas señaladas en el artículo 240 de este Código.

Modificación: Este artículo debería considerarse un parágrafo agravante dentro del artículo 239 del vigente Código penal colombiano, puesto que la figura que se maneja en este como hurto calificado y agravado se adapta a las necesidades provistas y no hay necesidad de crear un nuevo bien o apartado.

10.2.7. ***Artículo 269J: Transferencia no consentida de activos***. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Modificación: Este artículo debería considerarse de igual manera que el articulo 269I como un parágrafo agravante dentro del artículo 239 y tomando parte del artículo 246 del vigente Código penal colombiano, puesto que la figura que se maneja en el primero es hurto calificado y agravado y en el segundo artículo como estafa, lo que se adapta a las necesidades provistas y no hay necesidad de crear un nuevo bien o apartado.

10.2.8. ***Artículo 269K: Pornografía infantil por medios informáticos***. El que, con premeditación y valiéndose de engaños o cualquier medio de intimidación mediante el uso de dispositivos o sistemas informáticos o telemáticos adquiera, venda, distribuya, trafique, transmita, exhiba material de tipo pornográfico o cualquier tipo de manifestación de tipo sexual abusiva con menores de edad y que sean pertenecientes a circunstancias de vulnerabilidad o discapacidad, 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.

Adición: Se añade un nuevo artículo a la ley 1273 que contemple la pornografía infantil por medio del uso de sistemas informáticos y que sea sancionada no con penas administrativas como la ley 1336 de 2009 y 679 de 2001, sino que se considere penas agravantes de tipo penal para el que cometa este delito contra los menores de edad.

10.2.9. ***Artículo 269L: Falsificación de documentación digital***. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, por medio del uso de un dispositivo o programa informático o telemático; o adultere, incluya un documento no existente a un sistema de información o lo que haga sus veces, 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.

Adición: Se hace necesario adicionar un artículo que contemple la falsificación mediante el uso de dispositivos o programas de carácter informático, puesto que con ello se pone en riesgo la información contenida en un sistema de información de una organización. De esta manera se crea un artículo que refuerce las sanciones impuestas vigentes y que vincule el uso de las nuevas tecnologías y no solo se clasifique como falsificación de documento las firmas y certificados digitales, además se tiene presente las nuevas formas de contener información como las Tablet, celulares, entre otros.

11. PRESUPUESTO

11.1. RECURSO HUMANO

El recurso humano utilizado para este proyecto será un ingeniero de sistemas idóneo que será el mismo investigador, el cual tiene los conocimientos, habilidades y destrezas necesarias para desempeñar su labor en el área designada, además de poseer conocimientos amplios en el área de seguridad informática lo que hará posible el desarrollo y obtención de resultados esperados de la problemática planteada en este proyecto de investigación.

El investigador cumplirá con funciones de recolección de información y análisis de la misma, observará la realidad de su entorno y resolverá mediante la indagación y estudio de la hipótesis formulada con la ayuda de la organización sistémica de las diferentes actividades prestablecidas para cumplir con el alcance y objetivo del proyecto.

11.2. RECURSO TECNOLÓGICO

Para el desarrollo y cumplimiento de la presente monografía de investigación se utilizarán las siguientes herramientas tecnológicas:

- Un computador de escritorio propio con las siguientes características: capacidad de almacenamiento de 500 GB, monitor LG de 19'', procesador Pentium Dual- Core de 2.69 Hz, memoria RAM 3GB, sistema operativo Windows 7 Ultimate de 32 bits

- Internet cableado de banda ancha adquirido mediante el operador de servicio de internet contratado

- Memoria USB

- Software: paquete de aplicaciones de office 2010 (Word, Power point, etc.)

11.3. RECURSO MATERIAL

Dentro de los materiales físicos y digitales a utilizar para el desarrollo de la presente monografía de investigación son los siguientes:

- Copia del diario oficial No. 47.223 del 5 de enero de 2009 obtenido de la imprenta nacional
- Copia de las legislaciones escogidas en formato pdf obtenidas de las páginas oficiales de cada país
- Copia en formato pdf de las investigaciones, tesis, artículos y estudios obtenidos de páginas de repositorios o fuentes confiables

11.4. RECURSOS FINANCIEROS

Los costos para la realización del presente proyecto se tendrán en cuenta los siguientes costos presupuestados para el tiempo que dure la investigación en este caso un tiempo estimado de un semestre:

Tabla 7. Presupuesto

Ítem	Descripción	Valor mensual	Total (por 6 meses)
1	Internet	$42.000	$252.000
2	Servicio de Luz (este es un promedio mensual equivalente a 4 horas por día)	$30.000	$180.000
3	Papelería (impresiones, fotocopias, etc.)	$10.000	$60.000
4	Copia diario oficial No. 47.223 del 5 de enero de 2009 (Pago única vez)		$19.500

Tabla 7. (Continuación)

Ítem	Descripción	Valor mensual	Total (por 6 meses)
5	(*) Copia de legislaciones 3 US (Pago única vez) C/U		$27.591
6	Imprevistos (en caso de necesitar adquisición de material complementario)		$30.000
Total			$569.091

Fuente: El autor

(*) Nota: en este ítem se realiza la compra de las 3 legislaciones de los países seleccionados para realizar el comparativo, estas normativas de acuerdo al país tienen un costo aproximado de 3US que realizando la conversión a pesos colombianos es un equivalente a $9.197.

Los gastos mencionados en la tabla anterior, son el equivalente al costo total del análisis y desarrollo del proyecto de investigación.

12. CONCLUSIONES

Por la naturaleza del presente proyecto, el cual no es aplicado o hace parte de una investigación científica, sino que por el contrario es de carácter analítico a una norma estatuaria de una problemática de seguridad informática como lo son los delitos informáticos en Colombia, se omite en este caso el apartado de resultados y discusión.

✓ Dentro del desarrollo del presente proyecto se muestran y analizan las diversas técnicas de cibercriminalidad que se cometen con más frecuencia en Colombia, teniendo en cuenta el origen y evolución de las nuevas tecnologías en el área de la informática y las telecomunicaciones.

De esta forma, se observa la evolución en los métodos, técnicas o herramientas que pueden ser aplicaciones o dispositivos hardware que también se han desarrollado para facilitar la tarea de robo, suplantación, estafa y demás delitos que puedan estar clasificados dentro de la lista creciente de las nuevas formas criminales de atentar contra la confidencialidad, integridad y disponibilidad de la información como activo primordial, así mismo que atentan contra los bienes de tipo mueble e intangibles con valor económico de las personas que son víctimas de los ataques o delitos informáticos. Por lo que con el presente proyecto se demuestra que aún falta normatividad en Colombia que logre abarcar todos los ámbitos de seguridad informática y que pueda sancionar correctamente este tipo de incidentes, que dejan daños en todos los entornos de desarrollo y crecimiento del país.

✓ Se encontraron las similitudes y diferencias existentes dentro de la ley 1273 de 2009, realizando una comparación de la misma con las leyes de Venezuela, Chile y Argentina sobre el tratamiento a los delitos informáticos. En donde se identificó que a pesar de ser muy parecidas en su estructura, tipificación de delitos, sanciones y penas, la ley 1273 de 2009 difiere en varios puntos como; interceptación ilícita, fraude informático, pornografía infantil, ataques a la integridad del sistema, falsificación de documentos digitales, en donde ésta queda corta al tratar estos temas y a pesar del esfuerzo de realizar la tipificación correspondiente dentro de sus artículos no logra abarcar la temática y deja algunos de estos puntos por fuera, por ejemplo es el caso de la pornografía infantil, que como resultado del análisis hecho se demuestra que las sanciones impuestas en la ley 1339 de 2009 y 679 de 2001 creada para este delito son de

tipo administrativo y no penal, aparte que en las mismas no se contempla con claridad el uso de dispositivos o medios informáticos utilizados para cometer este delito, lo que si se contempla dentro de uno de los artículos de las leyes de los países escogidos para realizar la comparación.

De esta manera, se puede concluir que la ley 1273 de 2009 esta desactualizada en este sentido y se necesita un análisis por parte de las autoridades correspondientes, en donde se pueda contemplar su modificación para realizar las adiciones tanto de artículos como de contenido que pueda mejorarla y constituir un bien jurídico que vaya acorde con las necesidades en materia de ciberdelincuencia actuales, para lo cual se adiciona en este proyecto los artículos 269K “Pornografía infantil por medios informáticos” y 269L “Falsificación de documentación digital” en donde se hace una propuesta puntual para abarcar las temática faltantes en la vigente ley.

✓ Se realizó un análisis de las sentencias de ley SP1245-2015 y 34564 emitidas sobre la ley 1273 de 2009, dentro del marco de apoyo para continuar con el análisis de la evolución de la misma frente al constante crecimiento de los delitos informáticos en Colombia. Este análisis permitió determinar que en realidad en Colombia hacen falta muchas herramientas o bienes jurídicos, que puedan adaptarse a la constante evolución de la cibercriminalidad, sus técnicas y nuevos métodos.

Se logró identificar dentro de este contexto, que no solamente existen falencias y/o ambigüedades dentro de la ley 1273 de 2009, sino que también no es clara la competencia de las diferentes autoridades que pueden procesar las denuncias que se reciben a diario frente a esta problemática, así por ejemplo se puede decir, que falta capacitación a las autoridades o entes encargados y el diseño claro de un artículo de competencia que defina quien debe seguir el debido proceso en caso de hurto por medios informáticos o transferencia de activos, teniendo en cuenta el origen del lugar desde donde se comete el delito y el lugar donde se llega a ejecutar como tal. Por esta clase de circunstancias los procesos se pueden pasar de una autoridad a otra como se analizó en las sentencias dentro de este proyecto y de esta manera dejan la posibilidad de vencimiento de términos que pueda favorecer en ese caso al delincuente y no a la víctima.

✓ Se identificó la posibilidad de establecer si es totalmente necesario dejar como parte de la ley 1273 de 2009 los artículos 269I “Hurto por medios informáticos y semejantes” o si es mejor como se explicó en el apartado correspondiente dentro

del presente proyecto, si es necesario la creación de un parágrafo agravante dentro del artículo 239 y 240 del vigente código penal, puesto que esta figura se adapta como se analizó anteriormente a la comisión de delitos informáticos por medio de hurto. Así también se identificó la necesidad de crear el agravante para la transferencia de activos, debido a que los artículos vigentes del código penal se adaptan a esta figura como estafa y hurto calificado y agravado como se explica en el análisis realizado, de esta forma no sería necesario que estuviera como artículo propio dentro de la presente ley 1273.

✓ Se modificaron los artículos 269A, 269C, 269D, 269E, 269G de la ley 1273 de 2009, de acuerdo con los resultados obtenidos del análisis de las falencias y la comparación de la misma frente a las legislaciones latinoamericanas escogidas para ello. También se tuvo en cuenta la estadística desde el año 2013 hasta el año 2015 del número de denuncias recibidas en el país, el porcentaje de ocurrencia de las mismas, el artículo que se infringe de la legislación colombiana y del convenio de Budapest sobre los diferentes delitos informáticos lo que permite tener una referencia.

Por lo anteriormente expuesto, se puede confirmar y observar que la ley colombiana 1273, a pesar de haber sido creada para dar un tratamiento de carácter jurídico frente al flagelo de ciberdelincuencia sufrido actualmente, no es suficiente, ya que desde el año 2013 ha ido creciendo en todo el territorio nacional, por cuanto se debe pensarse en estrategias que fortalezcan el bien jurídico y a su vez integre las medidas que deben adoptarse en cuanto a seguridad informática se refiere, con el fin de reducir, prevenir o mitigar el daño causado por esta problemática.

✓ Se identifica la falta de un artículo de definiciones de los diferentes delitos informáticos dentro de la vigente ley 1273 de 2009, que pueda servir de referencia y consulta en el debido momento por las autoridades que tengan bajo su custodia algún proceso de un caso que contenga como materia probatoria un hecho cometido por delitos informáticos.

De esta manera, se creó un artículo de definiciones de los delitos informáticos más recurrentes dentro del presente proyecto como respuesta a esta falencia, permitiendo de esta manera fortalecer el bien jurídico analizado y como herramienta de consulta o referencia en el caso que se amerite, según sea contemplado por la autoridad competente, con ello se evitaría que cierto delitos

cometidos mediante el uso de aplicaciones o dispositivos informáticos sean juzgados por error de manera ordinaria saltándose la ley vigente para estos casos.

13. DIVULGACIÓN

El presente proyecto de investigación denominado “ANÁLISIS DE LA LEY 1273 DE 2009 Y LA EVOLUCIÓN DE LA LEY CON RELACIÓN A LOS DELITOS INFORMÁTICOS EN COLOMBIA”, tendrá como único medio de divulgación el repositorio institucional de la Universidad Nacional Abierta y a Distancia UNAD, en donde quedará como referencia de consulta para las personas externas y estudiantes de la universidad de los diferentes programas académicos de pregrado y posgrado.

BIBLIOGRAFIA

ABOGADOS PORTALEY MADRID PENAL, CIVIL E INTERNET (2015). Qué es y cómo combatir el cibercrimen {En línea} {20 de Abril de 2016} Disponible en http://portaley.com/2015/04/que-es-y-como-combatir-el-cibercrimen/#

ACUNIO DEL PINO, Santiago. Delitos informáticos: generalidades. Tipos de delitos informáticos Pág. 27- 31 {En línea} {20 de Abril de 2016} Disponible en http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

ARGENTINA. Ley 11.723 (23, Septiembre, 1933). Régimen legal de la propiedad intelectual. {En línea} {20 de Abril de 2016} Disponible en http://www.infoleg.gob.ar/infolegInternet/anexos/40000-44999/42755/texact.htm#1

--------. Ley 24.766 (20, Diciembre, 1996). Ley de confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales honestos {En línea} {20 de Abril de 2016} Disponible en http://www.infoleg.gob.ar/infolegInternet/anexos/40000-44999/41094/norma.htm

--------. Ley 25.326 (30, Octubre, 2000). Protección de los datos personales {En línea} {20 de Abril de 2016} Disponible en: http://www.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/texact.htm

--------. Ley 25.856 de 2003 (4, Diciembre, 2003). Consideración de la producción de software como actividad industrial {En línea} {20 de Abril de 2016} Disponible en http://www.infoleg.gov.ar/infolegInternet/anexos/90000-94999/91606/norma.htm

--------. Ley 25.922 (7, Septiembre, 2004). Ley de promoción de la industria del software {En línea} {20 de Abril de 2016} Disponible en: http://www.infoleg.gov.ar/infolegInternet/anexos/95000-99999/98433/norma.htm

--------.Ley 26.388 (24, Junio, 2008) Código penal Disponible en http://www.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm

ASOCIACIÓN ARGENTINA DE DERECHO DE ALTA TECNOLOGÍA. Delitos Informáticos Antecedentes Internacionales para una Legislación Nacional Proyectos Legislativos {En línea} {20 de Abril de 2016} Disponible en http://www.aadat.org/delitos_informaticos20.htm

CENTRO CIBERNÉTICO POLICIAL. Ciberincidentes {En línea} {23 de Octubre de 2016} Disponible en http://www.ccp.gov.co/ciberincidentes/tiempo-real/historico

CERT. (2001) Denial of Service Attacks. Software Engineering Institute. Carnegie Mellon. {En línea} {20 de Abril de 2016} Disponible en: www.cert.org/tech_tips/denial_of_service.html

CHILE. Ley 17.366 (2, Octubre, 1970). Propiedad intelectual {En línea} {22 de Abril de 2016} Disponible en http://www.leychile.cl/Navegar?idNorma=28933

--------. Ley 19.223 (7, Junio, 1993). Ley Relativa a delitos informáticos {En línea} {22 de Abril de 2016} Disponible en http://www.leychile.cl/Navegar?idNorma=30590

--------. Ley 19.628 (28, Agosto, 1999). Protección de datos de carácter personal {En línea} {22 de Abril de 2016} Disponible en http://www.leychile.cl/Navegar?idNorma=141599

--------. Ley 19.799 (12, Abril, 2002) Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma {En línea} {22 de Abril de 2016} Disponible en http://www.leychile.cl/Navegar?idNorma=196640

CARHUAMACA, D. Seguridad de la información: realidad o Utopía {En línea} {22 de Abril de 2016} Disponible en: http://www.monografias.com/trabajos85/seguridad-informacion-realidad-o-utopia/seguridad-informacion-realidad-o-utopia.shtml#ixzz43P7fBC32

COLOMBIA. MINISTERIO DEL INTERIOR Y DE JUSTICIA. Ley 1273 de 2009 (5, Enero, 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. Diario oficial Bogotá D.C., 2009 No 47.223 {En línea} {22 de Abril de 2016} Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

--------. Ley 1266 de 2008 (31, Diciembre, 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. Diario oficial Bogotá D.C., 2008 No 47219 {En línea} {22 de Abril de 2016} Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34488

--------. Ley 1336 de 2009 (21, Julio, 2009). 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. Diario oficial Bogotá D.C., 2009 No 47.417 {En línea} {22 de Abril de 2016} Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36877

-------. Ley 1437 de 2011 (18, Enero, 2011). Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo. Diario oficial Bogotá D.C., 2011 No 47.956 {En línea} {22 de Abril de 2016} Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=41249

--------. Ley 599 de 2000 (24, Julio, 2000). Por la cual se expide el Código Penal. Diario oficial Bogotá D.C., 2000 No 44097 {En línea} {25 de Abril de 2016} Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

--------. Ley Estatutaria 1581 de 2012 (17, Octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario oficial Bogotá D.C., 2012 No 48587 {En línea} {25 de Abril de 2016} Disponible enhttp://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

--------. Ley 446 de 1998 (7, Julio, 1998). Por la cual se adoptan como legislación permanente algunas normas del Decreto 2651 de 1991, se modifican algunas del Código de Procedimiento Civil, se derogan otras de la Ley 23 de 1991 y del Decreto 2279 de 1989, se modifican y expiden normas del Código Contencioso Administrativo y se dictan otras disposiciones sobre descongestión, eficiencia y acceso a la justicia. Diario oficial Bogotá D.C., 1998 No 43335 {En línea} {25 de Abril de 2016} Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3992

--------. Ley 600 de 2000 (24, Julio, 2000). Por la cual se expide el Código de Procedimiento Penal. Diario oficial Bogotá D.C., 2000 No 44097 {En línea} {25 de Abril de 2016} Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6389

COLOMBIA. MINISTRO DE TECNOLOGÍAS, DE LA INFORMACIÓN Y LAS COMUNICACIONES. Ley estatutaria 1581 DE 2012 (17, Octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario oficial Bogotá D.C., 2012 No 48587 {En línea} {27 de Abril de 2016} Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

--------. Decreto 1377 de 2013 (27, Junio, 2013). Por el cual se reglamenta parcialmente la Ley 1581 de 2012. Diario oficial Bogotá D.C., 2013 No 48834 {En línea} {27 de Abril de 2016} Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=53646

COLOMBIA. MINISTRO DE HACIENDA Y CRÉDITO PÚBLICO. Ley 679 de 2001 (3, Agosto, 2001). Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución. Diario oficial Bogotá D.C., 2000 No 44509 {En línea} {27 de Abril de 2016} Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=18309

-------. Ley 57 de 1985 (5, Junio, 1985). Por la cual se ordena la publicidad de los actos y documentos oficiales. Diario oficial Bogotá D.C., 1985 No 37056 {En línea} {27 de Abril de 2016} Disponible en http://www.unal.edu.co/una/docs/RL/Externa/Leyes/ley%2057%20de%201985.pdf

COLOMBIA. MINISTRO DE GOBIERNO. Ley 44 de 1993 (5, Febrero, 1993). Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944. Diario oficial Bogotá D.C., 1993 No 40.740 {En línea} {27 de Abril de 2016} Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=3429

--------. Decreto 1360 de 1989. (23, Junio, 1989). Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor. Diario oficial Bogotá D.C., 1989 No 38871 {En línea} {27 de Abril de 2016} Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=10575

COLOMBIA. MINISTERIO DE DESARROLLO ECONÓMICO. Ley 527 de 1999 (18, Agosto, 1999). 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. Diario oficial Bogotá D.C., 1999 No 43673 {En línea} {27 de Abril de 2016} Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276

CONGRESO DE LA REPÚBLICA DE COLOMBIA. ¿Qué es una ley? {En línea} {29 de Abril de 2016} Disponible en http://www.senado.gov.co/legales/item/11164-que-es-una-ley

COMPUTER FORENSIC RECOVERY LABS (2015). Delitos informáticos. Glosario {En línea} {19 de Noviembre de 2016} Disponible en http://www.delitosinformaticos.info/delitos_informaticos/glosario.html

CORTE SUPREMAS DE JUSTICIA (2015). Sala de casación penal. Sentencia SP1245-2015 {En línea} {12 de Octubre de 2016} Disponible en http://190.24.134.101/corte/wp-content/uploads/relatorias/pe/b1mar2015/SP1245-2015.pdf

CORTE SUPREMA DE JUSTICIA (2010). Sala de casación penal. Sentencia 34564 {En línea} {12 de Octubre de 2016} Disponible en http://es.slideshare.net/Alediaganet/sentencia-34564-25-08-10-competencia-transferencia-activos

COUNCIL OF EUROPE, (2016).Convention on Cybercrim CETS No.: 185. {En línea} {29 de Abril de 2016} Disponible en http://www.coe.int/es/web/conventions/home

Definición de derecho penal - Qué es, Significado y Concepto {En línea} {29 de Abril de 2016} Disponible en http://definicion.de/derecho-penal/#ixzz43PVvmiEK

Definición. Definición de legislación {En línea} {29 de Abril de 2016} Disponible en http://definicion.mx/legislacion/

GANDINI, I. Delta. Ley de los delitos informáticos en Colombia {En línea} {29 de Abril de 2016} Disponible en http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia

GARCÍA, C. (2010). Hacking ético. Hablemos de Spoofing {En línea} {19 de Noviembre de 2016} Disponible en https://hacking-etico.com/2010/08/26/hablemos-de-spoofing/

GOBIERNO DE ESPAÑA. Ministerio de educación, cultura y deporte. MONOGRÁFICO: Introducción a la seguridad informática - Seguridad de la información / Seguridad informática. Seguridad de la información / Seguridad informática {En línea} {29 de Abril de 2016} Disponible en http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1

GUZMÁN, A. (2011). Seguridad Informática. Confidencialidad e integridad {En línea} {29 de Abril de 2016} Disponible en http://seguridadanggie.blogspot.com.co/2011/11/confidencialidad.html

ICONTEC (2008). Norma Técnica Colombiana NTC 1486 {En línea} {29 de Abril de 2016} Disponible en: http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf

MANENT, M. Derecho.com. Violación de datos personales {En línea} {2 de Mayo de 2016} Disponible en http://www.derecho.com/c/Violaci%C3%B3n_de_datos_personales

NORTON (2016). Bots y botnets: Una amenaza creciente {En línea} {2 de Noviembre de 2016} Disponible en https://es.norton.com/botnet

POSADA MAYA, R. (2006). Aproximación a la criminalidad informática en Colombia. Revista de derecho, comunicaciones y nuevas tecnologías (2), págs 11-60

REMOLINA, A. (2009). Universidad de los Andes. Facultad de derecho. Relatores temáticos. La obtención y comercialización ilegal de datos personales es un delito: Ley 1273 de 2009 {En línea} {2 de Mayo de 2016} Disponible enhttps://relatorestematicos.uniandes.edu.co/index.php/proteccion-datos-personales/relatoria/131-ley-1273-de-2009.html

SEMANA (2014). ¿Qué es un Malware y cómo se puede prevenir? {En línea} {19 de Noviembre de 2016} Disponible en http://www.semana.com/tecnologia/tips/articulo/que-malware-como-puede-prevenir/372913-3

SEGU.INFO seguridad de la información. Keylogger {En línea} {19 de Noviembre de 2016} Disponibe en http://www.segu-info.com.ar/malware/keylogger.htm

OJEDA PÉREZ, Jorge; RINCÓN RODRIGUEZ, Fernando y ARIAS FLOREZ, Miguel. (2010). Delitos informáticos y entorno jurídico vigente en Colombia {En línea} {2 de Mayo de 2016} Disponible en http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003

TELLEZ VALDÉS, Julio. “Los Delitos informáticos. Situación en México”, Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO (2009). Eduteca. Manual para identificar y notificar phishing scam. Pharming {En línea} {19 de Noviembre de 2016} Disponible en http://www.seguridad.unam.mx/usuario-casero/eduteca/main.dsc?id=194

VENEZUELA. Ley especial contra los delitos informáticos (30, Octubre, 2001). Gaceta Oficial de la República Bolivariana de Venezuela No 37.313 {En línea} {2 de Mayo de 2016} Disponible en http://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

ANEXO A

LEGISLACIÓN COLOMBIANA SOBRE DELITOS INFORMÁTICOS

LEY 1273 DEL 5 DE ENERO 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.

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. 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.

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.

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.

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.

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.

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.

Artículo 269G: Suplantación de sitios web para capturar datos personales. 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, 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, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.

2. Por servidor público en ejercicio de sus funciones.

3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.

4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.

5. Obteniendo provecho para sí o para un tercero.

6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.

7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

CAPITULO II

De los atentados informáticos y otras infracciones

Artículo 269I: Hurto por medios informáticos y semejantes. 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, incurrirá en las penas señaladas en el artículo 240 de este Código.

Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

Si la conducta descrita en los dos incisos anteriores tuviere una cuantía superior a 200 salarios mínimos legales mensuales, la sanción allí señalada se incrementará en la mitad.

Artículo 2°. Adiciónese al artículo 58 del Código Penal con un numeral 17, así:

Artículo 58. Circustancias de mayor punibilidad. Son circunstancias de mayor punibilidad, siempre que no hayan sido previstas de otra manera:

(...)

17. Cuando para la realización de las conductas punibles se utilicen medios informáticos, electrónicos o telemáticos.

Artículo 3°. Adiciónese al artículo 37 del Código de Procedimiento Penal con un numeral 6, así:

Artículo 37. De los Jueces Municipales. Los jueces penales municipales conocen:

(...)

6. De los delitos contenidos en el título VII Bis.

Artículo 4°. La presente ley rige a partir de su promulgación y deroga todas las disposiciones que le sean contrarias, en especial el texto del artículo 195 del Código Penal.

ANEXO B

LEGISLACIÓN ARGENTINA SOBRE DELITOS INFORMÁTICOS

LEY 26388 DEL 4 DE JUNIO DE 2008

ARTÍCULO 1º — Incorpóranse como últimos párrafos del artículo 77 del Código Penal, los siguientes:

El término "documento" comprende toda representación de actos o hechos, con independencia del soporte utilizado para su fijación, almacenamiento, archivo o transmisión.

Los términos "firma" y "suscripción" comprenden la firma digital, la creación de una firma digital o firmar digitalmente.

Los términos "instrumento privado" y "certificado" comprenden el documento digital firmado digitalmente.

ARTICULO 2º — Sustitúyese el artículo 128 del Código Penal, por el siguiente:

Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

ARTICULO 3º — Sustitúyese el epígrafe del Capítulo III, del Título V, del Libro II del Código Penal, por el siguiente:

"Violación de Secretos y de la Privacidad"

ARTICULO 4º — Sustitúyese el artículo 153 del Código Penal, por el siguiente:

Artículo 153: Será reprimido con prisión de quince (15) días a seis (6) meses el que abriere o accediere indebidamente a una comunicación electrónica, una carta, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica, una carta, un pliego, un despacho u otro papel privado, aunque no esté cerrado; o indebidamente suprimiere o desviare de su destino una correspondencia o una comunicación electrónica que no le esté dirigida.

En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones provenientes de cualquier sistema de carácter privado o de acceso restringido.

La pena será de prisión de un (1) mes a un (1) año, si el autor además comunicare a otro o publicare el contenido de la carta, escrito, despacho o comunicación electrónica.

Si el hecho lo cometiere un funcionario público que abusare de sus funciones, sufrirá además, inhabilitación especial por el doble del tiempo de la condena.

ARTICULO 5º — Incorpórase como artículo 153 bis del Código Penal, el siguiente:

Artículo 153 bis: Será reprimido con prisión de quince (15) días a seis (6) meses, si no resultare un delito más severamente penado, el que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido.

La pena será de un (1) mes a un (1) año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

ARTICULO 6º — Sustitúyese el artículo 155 del Código Penal, por el siguiente:

Artículo 155: Será reprimido con multa de pesos un mil quinientos ($ 1.500) a pesos cien mil ($ 100.000), el que hallándose en posesión de una correspondencia, una comunicación electrónica, un pliego cerrado, un despacho telegráfico, telefónico o de otra naturaleza, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros.

Está exento de responsabilidad penal el que hubiere obrado con el propósito inequívoco de proteger un interés público.

ARTICULO 7º — Sustitúyese el artículo 157 del Código Penal, por el siguiente:

Artículo 157: Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

ARTICULO 8º — Sustitúyese el artículo 157 bis del Código Penal, por el siguiente:

Artículo 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

ARTICULO 9º — Incorpórase como inciso 16 del artículo 173 del Código Penal, el siguiente:

Inciso 16. El que defraudare a otro mediante cualquier técnica de manipulación informática que altere el normal funcionamiento de un sistema informático o la transmisión de datos.

ARTICULO 10. — Incorpórase como segundo párrafo del artículo 183 del Código Penal, el siguiente:

En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

ARTICULO 11. — Sustitúyese el artículo 184 del Código Penal, por el siguiente:

Artículo 184: La pena será de tres (3) meses a cuatro (4) años de prisión, si mediare cualquiera de las circunstancias siguientes:

1. Ejecutar el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;

2. Producir infección o contagio en aves u otros animales domésticos;

3. Emplear substancias venenosas o corrosivas;

4. Cometer el delito en despoblado y en banda;

5. Ejecutarlo en archivos, registros, bibliotecas, museos o en puentes, caminos, paseos u otros bienes de uso público; o en tumbas, signos conmemorativos, monumentos, estatuas, cuadros u otros objetos de arte colocados en edificios o lugares públicos; o en datos, documentos, programas o sistemas informáticos públicos;

6. Ejecutarlo en sistemas informáticos destinados a la prestación de servicios de salud, de comunicaciones, de provisión o transporte de energía, de medios de transporte u otro servicio público.

ARTICULO 12. — Sustitúyese el artículo 197 del Código Penal, por el siguiente:

Artículo 197: Será reprimido con prisión de seis (6) meses a dos (2) años, el que interrumpiere o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza o resistiere violentamente el restablecimiento de la comunicación interrumpida.

ARTICULO 13. — Sustitúyese el artículo 255 del Código Penal, por el siguiente:

Artículo 255: Será reprimido con prisión de un (1) mes a cuatro (4) años, el que sustrajere, alterare, ocultare, destruyere o inutilizare en todo o en parte objetos destinados a servir de prueba ante la autoridad competente, registros o documentos confiados a la custodia de un funcionario público o de otra persona en el interés del servicio público. Si el autor fuere el mismo depositario, sufrirá además inhabilitación especial por doble tiempo.

Si el hecho se cometiere por imprudencia o negligencia del depositario, éste será reprimido con multa de pesos setecientos cincuenta ($ 750) a pesos doce mil quinientos ($ 12.500).

ARTICULO 14. — Deróganse el artículo 78 bis y el inciso 1º del artículo 117 bis del Código Penal.

ARTICULO 15. — Comuníquese al Poder Ejecutivo.

Dada en la sala de sesiones del congreso argentino, en buenos aires, a los cuatro días del mes de junio del año dos mil ocho.

ANEXO C

LEGISLACIÓN CHILENA SOBRE DELITOS INFORMÁTICOS

LEY Nº 19.223 DEL 7 DE JUNIO DE 1993

TIPIFICA FIGURAS PENALES RELATIVAS A LA INFORMÁTICA

Teniendo presente que el H. Congreso Nacional ha dado su aprobación al siguiente

Proyecto de Ley:

"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.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado 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 cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República.

ANEXO D

LEGISLACIÓN VENEZOLANA SOBRE DELITOS INFORMÁTICOS

LEY ESPECIAL CONTRA LOS DLEITOS INFORMÁTICOS 30 DE OCTUBRE DE 2001

TÍTULO I

DISPOSICIONES GENERALES

Artículo 1. Objeto de la Ley. La presente Ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley.

Artículo 2. Definiciones. A efectos de la presente Ley, y cumpliendo con lo previsto en el artículo 9 de la Constitución de la República Bolivariana de Venezuela, se entiende por:

a) Tecnología de Información: rama de la tecnología que se dedica al estudio, aplicación y procesamiento de datos, lo cual involucra la obtención, creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, transmisión o recepción de información en forma automática, así como el desarrollo y uso del “hardware”, “firmware”, “software”, cualesquiera de sus componentes y todos los procedimientos asociados con el procesamiento de datos.

b) Sistema: cualquier arreglo organizado de recursos y procedimientos diseñados para el uso de tecnologías de información, unidos y regulados por interacción o interdependencia para cumplir una serie de funciones específicas, así como la combinación de dos o más componentes interrelacionados, organizados en un paquete funcional, de manera que estén en capacidad de realizar una función operacional o satisfacer un requerimiento dentro de unas especificaciones previstas.

c) Data (datos): hechos, conceptos, instrucciones o caracteres representados de una manera apropiada para que sean comunicados, transmitidos o procesados

por seres humanos o por medios automáticos y a los cuales se les asigna o se les puede asignar un significado.

d) Información: significado que el ser humano le asigna a la data utilizando las convenciones conocidas y generalmente aceptadas.

e) Documento: registro incorporado en un sistema en forma de escrito, video, audio o cualquier otro medio, que contiene data o información acerca de un hecho o acto capaces de causar efectos jurídicos.

f) Computador: dispositivo o unidad funcional que acepta data, la procesa de acuerdo con un programa guardado y genera resultados, incluidas operaciones aritméticas o lógicas.

g) Hardware: equipos o dispositivos físicos considerados en forma independiente de su capacidad o función, que conforman un computador o sus componentes periféricos, de manera que pueden incluir herramientas, implementos, instrumentos, conexiones, ensamblajes, componentes y partes.

h) Firmware: programa o segmento de programa incorporado de manera permanente en algún componente del hardware.

i) Procesamiento de datos o de información: realización sistemática de operaciones sobre data o sobre información, tales como manejo, fusión, organización o cómputo.

j) Seguridad: condición que resulta del establecimiento y mantenimiento de medidas de protección, que garanticen un estado de inviolabilidad de influencias o de actos hostiles específicos que puedan propiciar el acceso a la data de personas no autorizadas, o que afecten la operatividad de las funciones de un sistema de computación.

k) Virus: programa o segmento de programa indeseado que se desarrolla incontroladamente y que genera efectos destructivos o perturbadores en un programa o componente del sistema.

l) Tarjeta inteligente: rótulo, cédula o carnet que se utiliza como instrumento de identificación; de acceso a un sistema; de pago o de crédito, y que contiene data, información o ambas, de uso restringido sobre el usuario autorizado para portarla.

m) Contraseña (password): secuencia alfabética, numérica o combinación de ambas, protegida por reglas de confidencialidad, utilizada para verificar la autenticidad de la autorización expedida a un usuario para acceder a la data o a la información contenidas en un sistema.

n) Mensaje de datos: cualquier pensamiento, idea, imagen, audio, data o información, expresados en un lenguaje conocido que puede ser explícito o

secreto (encriptado), preparados dentro de un formato adecuado para ser transmitido por un sistema de comunicaciones.

Artículo 3. Extraterritorialidad. Cuando alguno de los delitos previstos en la presente Ley se cometa fuera del territorio de la República, el sujeto activo quedará sometido a sus disposiciones si dentro del territorio de la República se hubieren producido efectos del hecho punible, y el responsable no ha sido juzgado por el mismo hecho o ha evadido el juzgamiento o la condena por tribunales extranjeros.

Artículo 4. Sanciones. Las sanciones por los delitos previstos en esta Ley serán principales y accesorias. Las sanciones principales concurrirán con las penas accesorias y ambas podrán también concurrir entre sí, de acuerdo con las circunstancias particulares del delito del cual se trate, en los términos indicados en la presente Ley.

Artículo 5. Responsabilidad de las personas jurídicas. Cuando los delitos previstos en esta Ley fuesen cometidos por los gerentes, administradores, directores o dependientes de una persona jurídica, actuando en su nombre o representación, éstos responderán de acuerdo con su participación culpable. La persona jurídica será sancionada en los términos previstos en esta Ley, en los casos en que el hecho punible haya sido cometido por decisión de sus órganos, en el ámbito de su actividad, con sus recursos sociales o en su interés exclusivo o preferente.

TÍTULO II

DE LOS DELITOS

Capítulo I

De los Delitos Contra los Sistemas que Utilizan Tecnologías de Información.

Artículo 6. 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, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

Artículo 7. 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, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Incurrirá en la misma pena quien destruya, dañe, modifique o inutilice la data o la información contenida en cualquier sistema que utilice tecnologías de información o en cualesquiera de sus componentes.

La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias, si los efectos indicados en el presente artículo se realizaren mediante la creación, introducción o transmisión intencional, por cualquier medio, de un virus o programa análogo.

Artículo 8. 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.

Artículo 9. Acceso indebido o sabotaje a sistemas protegidos. Las penas previstas en los artículos anteriores se aumentarán entre una tercera parte y la mitad, cuando los hechos allí previstos o sus efectos recaigan sobre cualesquiera de los componentes de un sistema que utilice tecnologías de información protegido por medidas de seguridad, que esté destinado a funciones públicas o que contenga información personal o patrimonial de personas naturales o jurídicas.

Artículo 10. 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, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Artículo 11. 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 cualesquiera de sus componentes, será penada

con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

La pena se aumentará de un tercio a la mitad, si el delito previsto en el presente artículo se cometiere con el fin de obtener algún tipo de beneficio para sí o para otro.

El aumento será de la mitad a dos tercios, si se pusiere en peligro la seguridad del Estado, la confiabilidad de la operación de las instituciones afectadas o resultare algún daño para las personas naturales o jurídicas, como consecuencia de la revelación de las informaciones de carácter reservado.

Artículo 12. 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, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

Cuando el agente hubiere actuado con el fin de procurar para sí o para otro algún tipo de beneficio, la pena se aumentará entre un tercio y la mitad.

El aumento será de la mitad a dos tercios si del hecho resultare un perjuicio para otro.

Capítulo II

De los Delitos Contra la Propiedad

Artículo 13. 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, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 14. 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, será penado con prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.

Artículo 15. Obtención indebida de bienes o servicios. Quien, sin autorización para portarlos, utilice una tarjeta inteligente ajena o instrumento destinado a los mismos fines, o el que utilice indebidamente tecnologías de información para requerir la obtención de cualquier efecto, bien o servicio; o para proveer su pago sin erogar o asumir el compromiso de pago de la contraprestación debida, será castigado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 16. Manejo fraudulento 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, será penada con prisión de cinco a diez años y multa de quinientas a mil unidades tributarias.

En la misma pena incurrirá quien, sin haber tomado parte en los hechos anteriores, adquiera, comercialice, posea, distribuya, venda o realice cualquier tipo de intermediación de tarjetas inteligentes o instrumentos destinados al mismo fin, o de la data o información contenidas en ellos o en un sistema.

Artículo 17. Apropiación de tarjetas inteligentes o instrumentos análogos. 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, será penado con prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.

La misma pena se impondrá a quien adquiera o reciba la tarjeta o instrumento a que se refiere el presente artículo.

Artículo 18. Provisión indebida de bienes o servicios. Todo aquel que, a sabiendas de que una tarjeta inteligente o instrumento destinado a los mismos fines, se encuentra vencido, revocado; se haya indebidamente obtenido, retenido, falsificado, alterado; provea a quien los presente de dinero, efectos, bienes o servicios, o cualquier otra cosa de valor económico será penado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 19. Posesión de equipo para falsificaciones. Todo aquel que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos, reciba, adquiera, posea, transfiera, comercialice, distribuya, venda, controle o custodie cualquier equipo de fabricación de tarjetas inteligentes o de instrumentos destinados a los mismos fines, o cualquier equipo o componente que capture, grabe, copie o transmita la data o información de dichas tarjetas o instrumentos, será penado con prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.

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. Toda persona que intencionalmente se apodere, utilice, modifique o elimine por cualquier medio, sin el consentimiento de su dueño, la data o información personales de otro o sobre las cuales tenga interés legítimo, que estén incorporadas en un computador o sistema que utilice tecnologías de información, será penada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

La pena se incrementará de un tercio a la mitad si como consecuencia de los hechos anteriores resultare un perjuicio para el titular de la data o información o para un tercero.

Artículo 21. Violación de la privacidad de las comunicaciones. Toda persona que mediante el uso de tecnologías de información acceda, capture, intercepte, interfiera, reproduzca, modifique, desvíe o elimine cualquier mensaje de datos o señal de transmisión o comunicación ajena, será sancionada con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 22. Revelación indebida de data o información de carácter personal. Quien revele, difunda o ceda, en todo o en parte, los hechos descubiertos, las imágenes, el audio o, en general, la data o información obtenidos por alguno de los medios indicados en los artículos 20 y 21, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Si la revelación, difusión o cesión se hubieren realizado con un fin de lucro, o si resultare algún perjuicio para otro, la pena se aumentará de un tercio a la mitad.

Capítulo IV

De los Delitos Contra Niños, Niñas o Adolescentes

Artículo 23. Difusión o exhibición de material pornográfico. Todo aquel que, por cualquier medio que involucre el uso de tecnologías de información, exhiba, difunda, transmita o venda material pornográfico o reservado a personas adultas, sin realizar previamente las debidas advertencias para que el usuario restrinja el acceso a niños, niñas y adolescentes, será sancionado con prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.

Artículo 24. Exhibición pornográfica de niños o adolescentes. Toda persona que por cualquier medio que involucre el uso de tecnologías de información, utilice a la persona o imagen de un niño, niña o adolescente con fines exhibicionistas o pornográficos, será penada con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Capítulo V

De los Delitos Contra el Orden Económico

Artículo 25. Apropiación de propiedad intelectual. Quien sin autorización de su propietario y con el fin de obtener algún provecho económico, reproduzca, modifique, copie, distribuya o divulgue un software u otra obra del intelecto que haya obtenido mediante el acceso a cualquier sistema que utilice tecnologías de información, será sancionado con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias.

Artículo 26. Oferta engañosa. Toda persona que ofrezca, comercialice o provea de bienes o servicios, mediante el uso de tecnologías de información, y haga alegaciones falsas o atribuya características inciertas a cualquier elemento de dicha oferta, de modo que pueda resultar algún perjuicio para los consumidores, será sancionada con prisión de uno a cinco años y multa de cien a quinientas unidades tributarias, sin perjuicio de la comisión de un delito más grave.

TÍTULO III

DISPOSICIONES COMUNES

Artículo 27. Agravantes. La pena correspondiente a los delitos previstos en la presente Ley se incrementará entre un tercio y la mitad:

1. Si para la realización del hecho se hubiere hecho uso de alguna contraseña ajena indebidamente obtenida, quitada, retenida o que se hubiere perdido.

2. Si el hecho hubiere sido cometido mediante el abuso de la posición de acceso a data o información reservada, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función.

Artículo 28. Agravante especial. La sanción aplicable a las personas jurídicas por los delitos cometidos en las condiciones señaladas en el artículo 5 de esta Ley, será únicamente de multa, pero por el doble del monto establecido para el referido delito.

Artículo 29. Penas accesorias. Además de las penas principales previstas en los capítulos anteriores, se impondrán, necesariamente sin perjuicio de las establecidas en el Código Penal, las penas accesorias siguientes:

1. El comiso de equipos, dispositivos, instrumentos, materiales, útiles, herramientas y cualquier otro objeto que hayan sido utilizados para la comisión de los delitos previstos en los artículos 10 y 19 de la presente Ley.

2. El trabajo comunitario por el término de hasta tres años en los casos de los delitos previstos en los artículos 6 y 8 de esta Ley.

3. La inhabilitación para el ejercicio de funciones o empleos públicos; para el ejercicio de la profesión, arte o industria; o para laborar en instituciones o empresas del ramo por un período de hasta tres (3) años después de cumplida o

conmutada la sanción principal, cuando el delito se haya cometido con abuso de la posición de acceso a data o información reservadas, o al conocimiento privilegiado de contraseñas, en razón del ejercicio de un cargo o función públicas, del ejercicio privado de una profesión u oficio, o del desempeño en una institución o empresa privada, respectivamente.

4. La suspensión del permiso, registro o autorización para operar o para el ejercicio de cargos directivos y de representación de personas jurídicas vinculadas con el uso de tecnologías de información, hasta por el período de tres (3) años después de cumplida o conmutada la sanción principal, si para cometer el delito el agente se hubiere valido o hubiere hecho figurar a una persona jurídica.

Artículo 30. Divulgación de la sentencia condenatoria. El Tribunal podrá además, disponer la publicación o difusión de la sentencia condenatoria por el medio que considere más idóneo.

Artículo 31. Indemnización Civil. En los casos de condena por cualquiera de los delitos previstos en los Capítulos II y V de esta Ley, el juez impondrá en la sentencia una indemnización en favor de la víctima por un monto equivalente al daño causado.

Para la determinación del monto de la indemnización acordada, el juez requerirá del auxilio de expertos.

TÍTULO IV

DISPOSICIONES FINALES

Artículo 32. Vigencia. La presente Ley entrará en vigencia, treinta días después de su publicación en la Gaceta Oficial de la República Bolivariana de Venezuela.

Artículo 33. Derogatoria. Se deroga cualquier disposición que colida con la presente Ley. Dada, firmada y sellada en el Palacio Federal Legislativo, sede de la Asamblea Nacional, en Caracas a los cuatro días del mes de septiembre de dos mil uno. Año 191° de la Independencia y 142° de la Federación.

ANEXO E

RESUMEN ANALÍTICO ESPECIALIZADO (RAE)

Título de Documento	ANÁLISIS DE LA LEY 1273 DE 2009 Y LA EVOLUCIÓN DE LA LEY CON RELACIÓN A LOS DELITOS INFORMÁTICOS EN COLOMBIA
Autor	SÁNCHEZ, Zulay
Palabras Claves	Delitos informáticos, seguridad informática, ley 1273 de 2009
Descripción Monografía de investigación para optar el título de especialista en seguridad informática. El presente documento se realiza con el fin de revisar e identificar las falencias y/o ambigüedades de la Ley 1273 de 2009 "De la protección de la información y de los datos" frente a la problemática de delitos informáticos en Colombia	
Fuentes Bibliográficas	Infoleg. (2008). Ley 26.388 Código penal. Buenos Aires, Argentina. Recuperado de http://www.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm Biblioteca del congreso nacional de Chile. (1993). Ley 19.223 Ley Relativa a delitos informáticos. Santiago, Chile. Recuperado de http://www.leychile.cl/Navegar?idNorma=30590 Diario oficial Bogotá D.C., No 47.223. (2009). Ley 1273 de 2009 De la protección de la información y de los datos Recuperado de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492 Gaceta Oficial de la República Bolivariana de Venezuela No 37.313. (2001). Ley especial contra los delitos informáticos. Recuperado de http://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf

Contenido:	

El presente proyecto describe la problemática de los delitos informáticos en Colombia, que desde la aparición de los mismos, ha afectado considerablemente el uso y transmisión de la información como activo en los diferentes procesos de las empresas y su crecimiento con calidad y eficacia en el mercado. Por esta razón, en 2009 se crea un bien jurídico que contempla un castigo penal y sanciones de tipo económico a las personas que cometan delitos contra la información y los datos personales mediante la manipulación de medios o dispositivos informáticos, sin embargo este bien jurídico lleva 7 años en vigencia sin presentar modificaciones que lo adapten al constante crecimiento de la delincuencia cibernética y aparición de nuevas técnicas de delitos informáticos.

Por consiguiente, con el desarrollo de la presente monografía de investigación se quiere identificar los vacíos existentes en la legislación nacional frente a la legislación internacional por medio del análisis y revisión de la ley 1273 de 2009, en miras de lograr una adecuada clasificación de los delitos informáticos que contribuya a formular propuestas efectivas para combatir los mismos. Para lo que se requiere como primer paso realizar un análisis de la evolución de los delitos informáticos frente al actual marco legislativo internacional y la ley 1273 Colombiana, además de realizar la consulta de la legislación contra los delitos informáticos de Argentina, Venezuela y Chile, países que se escogieron dentro del marco de la presente investigación como referencia latinoamericana de la legislación adoptada para hacer frente a la problemática descrita, con el fin de realizar un comparativo frente a la Ley 1273 para determinar las similitudes y diferencias existentes, como punto de referencia a la posible mejora de la legislación colombiana.

En segunda medida, se realiza un análisis de las sentencias de ley emitidas en cumplimiento de la Ley 1273 que permitan determinar las posibles falencias o ambigüedades de la misma.

Dentro del presente proyecto se analizó la evolución de los delitos informáticos en Colombia, mediante la investigación de documentación que permitió identificar la aparición de la comisión de los mismos en el país, con ello determinar su nivel de incidencia en los diferentes campos de desarrollo y a su vez hacer la revisión y posterior análisis frente a la ley 1273 de 2009, la cual hace parte de la modificación realizada al código penal colombiano en su titulo VII BIS, en busca de la clasificación y penalización de los hechos delictivos que contemplen el daño a la

información en alguno de su principios como la integridad, disponibilidad y confidencialidad.

Por consiguiente, se analiza esta problemática mediante el número de denuncias y su correspondiente porcentaje sobre delitos informáticos en el país, mediante las estadísticas que genera el centro cibernético de la policía nacional como parte de los organismos que vigila y busca proteger de este flagelo a los ciudadanos. Como otra medida para obtener resultados sobre la falencia y/o ambigüedades de la presente ley 1273 de 2009, se tomaron como referencia las sentencias SP1245-2015 y 34564 de 2010, las cuales muestran con claridad las dificultades de competencia, clasificación y definición de los delitos por medios informáticos a castigar, haciendo especial énfasis en demostrar que a pesar de tener un bien jurídico que penaliza estos hechos, no es posible lograr identificar y separar los mismos de los delitos que se describen como ordinarios o comunes, lo que genera una particular dificultad a la hora de realizar una definición jurídica acorde por parte de las autoridades perjudicando en muchos casos a la victima y dejando en impunidad o libertad según sea el caso al criminal.

Por otro lado, se realizó un comparativo de las leyes emitidas y que están vigentes sobre delitos informáticos de los países latinoamericanos escogidos frente a la ley colombiana 1273 de 2009, en donde se identificaron las ambigüedades y falencias de la misma y se pudo establecer una serie de propuestas puntuales dentro de los artículos que se contemplan en la misma, en donde se modifican algunos de ellos con el fin de mejorar el bien jurídico, así mismo se adicionaron dos artículos nuevos que contemplen delitos que se lograron identificar como faltantes en la ley vigente y un artículo de definiciones de los delitos informáticos más recurrentes, con el fin que sirva como guía de consulta a las autoridades judiciales o competentes para la penalización de los mismos.

De esta manera, se logra contribuir con propuestas específicas como es el principal objetivo del presente proyecto a la mejora de la legislación Colombiana contrarrestando la problemática de seguridad informática y de protección de datos actual.

Metodología

El presente proyecto es una monografía de investigación, debido a que es un tema en desarrollo y no hay una línea base de investigación sobre el tema escogido. Por otro lado, se tomó como herramienta de recolección y análisis de información el análisis documental, ya que por medio del mismo se logró estudiar y analizar a

fondo la problemática basándose en las normas legislativas existentes que hacen referencia al tema.

Conclusiones

✓ Se adiciona en este proyecto los artículos 269K “Pornografía infantil por medios informáticos” y 269L “Falsificación de documentación digital” en donde se hace una propuesta puntual para abarcar las temática faltantes en la vigente ley.

✓ Se realizó un análisis de las sentencias de ley SP1245-2015 y 34564 emitidas sobre la ley 1273 de 2009, dentro del marco de apoyo para continuar con el análisis de la evolución de la misma frente al constante crecimiento de los delitos informáticos en Colombia. Este análisis permitió determinar que en realidad en Colombia hacen falta muchas herramientas o bienes jurídicos, que puedan adaptarse a la constante evolución de la cibercriminalidad, sus técnicas y nuevos métodos.

✓ Se modificaron los artículos 269A, 269C, 269D, 269E, 269G de la ley 1273 de 2009, de acuerdo con los resultados obtenidos del análisis de las falencias y la comparación de la misma frente a las legislaciones latinoamericanas escogidas para ello

✓ Se creó un artículo de definiciones de los delitos informáticos más recurrentes dentro del presente proyecto como respuesta a esta falencia, permitiendo de esta manera fortalecer el bien jurídico analizado y como herramienta de consulta o referencia en el caso que se amerite, según sea contemplado por la autoridad competente, con ello se evitaría que cierto delitos cometidos mediante el uso de aplicaciones o dispositivos informáticos sean juzgados por error de manera ordinaria saltándose la ley vigente para estos casos

Recomendaciones.

Se requiere de una revisión y análisis de las leyes y normas colombianas frente a la protección de datos y de la información, con el fin de salvaguardar la misma y contemplar medidas o estrategias que permitan un buen uso de la información y de las nuevas tecnologías, así también proponer sanciones que vayan acordes a la problemática.

Es necesario impartir desde el nivel nacional políticas de seguridad informática que puedan adaptarse a las necesidades de las empresas colombianas y así mismo en cada una de ellas dar la capacitación necesaria a sus funcionarios para poder implementarlas y lograr mitigar, prevenir o corregir los daños causados por

los delitos informáticos.