ANÁLISIS COMPARATIVO SOBRE DELITOS INFORMÁTICOS EN COLOMBIA CON RELACIÓN A SEIS PAÍSES DE LATINOAMÉRICA

ANDRES BOLAÑOS DIAZ
1.085.257.698

TERESA DE JESUS NARVAEZ NARVAEZ
59.830.899

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
SAN JUAN DE PASTO
2014

ANÁLISIS COMPARATIVO SOBRE DELITOS INFORMÁTICOS EN COLOMBIA CON RELACIÓN A SEIS PAÍSES DE LATINOAMÉRICA

ANDRES BOLAÑOS DIAZ
1.085.257.698

TERESA DE JESUS NARVAEZ NARVAEZ
59.830.899

Monografía para optar el título de
Especialistas en Seguridad Informática

Ing. WILSON CASTAÑOGALVIZ
Asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA "UNAD"
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
SAN JUAN DE PASTO
2014

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

_____

_____

_____

ING. GABRIEL MAURICIO RAMIREZ

_____

MSC.ING.CARLOS ALBERTO AMAYA TARAZONA

San Juan de Pasto, Octubre 17 de 2014

Este proyecto de grado está dedicado a mis padres que gracias a Dios los tengo a mi lado ya que ellos fueron los que me regalaron la vida, que quienes con mucho amor y cariño han logrado formar una gran persona, como hijo, esposo y profesional para la sociedad.

A mi esposa, que ha estado a mi lado incondicionalmente brindándome cariño, confianza y apoyo de un forma desinteresada para lograr esta etapa de mi vida como especialista, a mi hijo Andrés Felipe que es el motivo y la razón que ha llevado a seguir superándome cada día más para ser su ejemplo en su vida que apenas empieza.

Andrés Bolaños Díaz

"Al único que nos salva por medio
de Cristo Jesús nuestro Señor,
a Él sea gloria, honor, fuerza y poder
desde antes de todos los tiempos,
ahora y por todos los siglos. Amén".
Judas 1:22.
Dios mío eres todo para mí!
Teresa Narváez N.

AGRADECIMIENTOS

Los autores expresan sus agradecimientos:

Al Alto y Sublime Dios Todopoderoso por su grande fidelidad, todo el tiempo ha estado alentando nuestro caminar. Al Señor Jesucristo, por ser el principal director y gestor de éste trabajo sin Él nada de esto hubiese sido posible, pues es la luz que ilumina el entendimiento. (Autora: Teresa Narváez.)

A Teresa Narváez por ser mí compañera de proyecto de grado y ante todo mi amiga, sin su ayuda hubiese sido muy difícil lograrlo, a pesar del poco tiempo que la he conocido es una profesional de muchas cualidades y grandiosa personalidad. Gracias a Dios logramos terminar el proyecto con todas las modificaciones solicitadas por los jurados asignados. (Autor: Andrés Bolaños.)

A la Universidad Nacional a Distancia “UNAD”, por ser el medio por el cual se forjan profesionales para la vida.

Al Ingeniero Wilson Castaño Galvis, por la disposición y profesionalismo con que asesoró éste trabajo de grado.

A nuestros familiares y amigos que brindaron apoyo incondicional y fortaleza en los momentos difíciles.

Y a cada persona que estuvo involucrada en el desarrollo de éste trabajo de grado, muchas gracias y que Dios los bendiga.

CONTENIDO

Pág.

LISTA DE CUADROS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

Bullying: Intimidación o acoso, es la práctica de actos violentos, intencionales y repetidos, contra una persona indefensa, causando daños físicos y psicológicos. El término viene del inglés "bully" que significa tirano, brutal. La violencia es cometida por una o más personas, con el propósito de intimidar o agredir a la víctima.[1]

Interpol:(Abreviaturade*OrganizaciónInternacionaldePolicíaCriminal*) Organización fundada en Viena en 1923 y reestructurada en 1946, con sede en París. Persigue los delitos cuando un criminal, burlando la policía de su país, pasa a país extranjero.[2]

Mobbing: Situación en la que una persona ejerce una violencia psicológica extrema, de forma sistemática y recurrente y durante un tiempo prolongado sobre otra persona o personas en el lugar de trabajo con la finalidad de destruir las redes de comunicación de la víctima o víctimas, destruir su reputación, perturbar el ejercicio de sus labores y lograr que finalmente esa persona o personas acaben abandonando el lugar de trabajo[3].

Monografía: Es una investigación de carácter bibliográfico a la cual se lepueden adicionar citas testimoniales en caso de que el tema lo requiera, que apartir de una indagación crítica del estado del arte, sistematiza soluciones oenfoques para abordar problemas del entorno o áreas temáticas de frontera enel currículo de un programa formal.[4] Un tipo de Monografía es la de Investigación, donde se realiza una investigación propia, se aportan hallazgos, y se recomiendan nuevos puntos de vista[5].

Phishing: Consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude.Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas. De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos del estafador.[6]

---

[1]Significados. (2013). *Significado de Bullying.* Recuperado de http://www.significados.com/bullying/.
[2]The Free Dictionary. (2009). Recuperado de: http://es.thefreedictionary.com/Interpol .
[3]Universia. (1990). *¿Qué es el Mobbing?*.Recuperado de http://contenidos.universia.es/especiales../mobbing/concepto/index.htm.
[4]García Y, Gamboa M. (2011). *Lineamientos para Trabajos de Grado*. Bogotá D.C. Universidad Nacional Abierta y a Distancia – UNAD.
[5]Alvarado E., Borges, B. (2004). *Transcripción Guía práctica para el desarrollode monografías, ensayos, bibliografías y extractos*. Puerto Rico. Publicaciones Puertorriqueñas.
[6]Panda Security (2014). *Phishing.* Recuperado de: http://www.pandasecurity.com/colombia/homeusers/security-info/cybercrime/phishing/ .

Punitivo: Castigable.

Spam: Son aquellos mensajes que no han sido solicitados, es decir, son de destinatarios desconocidos a los cuales nosotros no hemos contactado. Si bien la principal vía de llegada de estos mensajes es a través del correo electrónico, también puede difundirse por otras vías, por ejemplo, a través de los teléfonos celulares. También denominado correo basura o mensaje basura.[7]

[7]Definición abc. (2007). *Definición de Spam.* Recuperado de: http://www.definicionabc.com/tecnologia/spam.php#ixzz3FJxSqofj.

RESUMEN DEL ESTUDIO

PROGRAMA ACADEMICO	:	Especialización en Seguridad Informática
AUTORES	:	Andrés Bolaños Díaz Teresa de Jesús Narváez Narváez
ASESOR	:	Ing. Wilson Castaño Galvis

TITULO: Análisis comparativo sobre delitos informáticos en Colombia con relación a seis países de Latinoamérica.

RESUMEN:

En la presente Monografía se realiza un análisis comparativo sobre delitos informáticos teniendo en cuenta la legislación encontrada sobre este tema en Colombia primeramente, Argentina, Costa Rica, Chile, Ecuador, Perú y Venezuela.

Se confrontanlas leyes de Delitos Informáticos de los países seleccionados con los delitos informáticos contemplados en el Convenio de Ciberdelincuencia de Budapest[8] que se acordó en el 2001 por la ONU (Organización de Naciones Unidas) de ese entonces, hoy ratificado por más de 100 países. Después de esto se hace una confrontación de cada artículo de la Legislación Colombiana Ley 1273 de 2009 comparada con las leyes que contemplan características similares de los 6 países seleccionados para el estudio: Argentina, Costa Rica, Chile, Ecuador, Perú y Venezuela; mediante esta comparación se determinarán fortalezas, debilidades y falencias de la legislación Colombiana en cuanto a los delitos informáticos, se establece un punto de vista por los Autores desde el conocimiento adquirido en el programa de Especialización de Seguridad Informática, y se concluye planteando mejoras que se pueden convertir en objeto de estudio para presentar proyectos de ley que permitan fortalecer la legislación Colombiana en el aspecto de brindar mayor protección a la ciudadanía en contra de los ciberdelincuentes que hoy en día abundan en la comunidad del ciberespacio.

PALABRAS CLAVE: Ley, Legislación, Ciberdelincuencia, Delito Informático, Sanciones legislativas, falencias, normativa.

[8]Serie de Tratados Europeos-n° 185. *Convenio sobre la Ciberdelincuencia.* Budapest, Concilio de Europa.

INTRODUCCION

Para un país la información y los datos, así como la tecnología que la soporta, representa uno de los activos más valiosos por lo tanto se debe velar por su preservación, respeto y protección, esto lo hace mediante la legislación.

En el estudio a continuación se realiza una comparación entre la legislación sobre Delitos Informáticos de 6 países seleccionados de América Latina con la Legislación Colombiana,para identificar las fortalezas, debilidades, falencias y sugerencias que se pueden aplicar para posteriores estudios de actualización o presentación de nuevos proyectos de ley que permitan la creación de nuevos artículos o modificación que fortalezcan la Constitución Nacional.

Han sido muchos los avances que la informática ha traído en la actualidad y consigo las diferentes formas de delitos que hacen uso de la informática, es así como las leyes internacionales como nacionales debieron implementar su departamento judicial con medidas sancionatorias para poder juzgar y tipificar este tipo de delitos, es necesario que los países se concentren en emitir soluciones jurídicas para contrarrestar este tipo de delitos que cambian constantemente; por esta razón la presente monografía explica algunos delitos bajo la luz del Convenio de Ciberdelincuencia de 2001[9], en el que se definieron los Delitos Informáticos que hoy en día son la base de muchas legislaciones a nivel mundial.

En primer lugar se hará una asociación de los delitos base del Convenio de Ciberdelincuencia con la legislación de cada país seleccionado para establecer el grado de cumplimiento de cada uno respecto a este convenio, luego se realizarán comparaciones específicas de la Ley 1273 de Enero 05 de 2009 con las normas de los seis países de la muestra para determinar las falencias y con ello se establece un planteamiento de mejora de la misma legislación.

[9]Serie de Tratados Europeos-n° 185. *Convenio sobre la Ciberdelincuencia*. Budapest, Concilio de Europa.

1. JUSTIFICACION

Actualmente los delitos informáticos han aumentado considerablemente al punto de ser necesario legislarlos para que tengan una justa penalización que pueda controlar su difusión y crecimiento. Se debe conocer el panorama de la legislación nacional e internacional en contra de los delitos informáticos para dimensionar la problemática que está afectando a Colombia y a países que se pueden encontrar en las mismas condiciones.

Las normas deben repasarse continuamente bajo un marco internacional para que se creen alternativas que puedan favorecer su mejor aplicabilidad y sean óptimas en el control de los delitos. Se debe propender porque estas normas abarquen la mayor parte de manifestación de un hecho delictivo, y máxime si se tienen lineamientos establecidos por países más desarrollados en la lucha por frenar este fenómeno ofensivo.

El presente monografía se desarrolla para determinar las falencias existentes en la legislación Colombiana en cuanto a delitos informáticos con respecto a seis países de Latinoamérica, entre los cuales están, Argentina, Costa Rica, Chile, Ecuador, Perúy Venezuela, bajo los lineamientos del Convenio de Ciberdelincuencia[10] de 2001, porque un Especialista de Seguridad Informática necesita conocer la posición que ha tomado su país en la defensa y preservación integral de los sistemas informáticos en contra de los ciberdelincuentes. En este orden de ideas, se hace necesario someter la normativa vigente a revisión para que se puedan determinar faltantes que motiven la formulación de nuevos proyectos de ley que permitan fortalecer la legislación que garantice la protección a los datos.Mediante la comparación se pueden extraer puntos clave sobre los cuales se puede actuar.

Como individuos, y desde cualquier campo de la ciencia, cada colombiano está llamado a realizar aportes que contribuyan al fortalecimiento del sistema jurídico, y desde la Ingeniería de Sistemas, aún más, desde el punto de vista de los Especialistas en Seguridad Informática debe existir una preocupación más alta por formular alternativas de mejora a la normatividad.

[10]Serie de Tratados Europeos-n° 185. *Convenio sobre la Ciberdelincuencia.* Budapest, Concilio de Europa.

2. DEFINICION DEL PROBLEMA

2.1DESCRIPCIÓN DEL PROBLEMA

En Colombia se ha creado un marco jurídico que abarca determinados delitos informáticos pero es necesario que se hagan aportes críticos que puedan motivar la creación de nuevos artículos legislativos que incorporen los delitos que aún no han sido contemplados en la legislación nacional. La norma se mantiene en un ambiente dinámico que permite su renovación y reforma, de modo que es posible argumentar la inclusión de normas que castiguen los nuevos delitos al identificarlos, con el fin de propender por la defensade la integridad de los datos y la información de la sociedad en general.

Un principio legislativo dice que no existe delito sí para ello no existe sanción, es decir, se puede realizar una acción mientras no esté sancionada en la Ley, por ello es necesario que se identifiquen las acciones que pueden estar afectando al individuo o sociedad y que estas acciones sean catalogadas como delito para que sobre ellas se impongan sanciones.

Los delitos informáticos fueron catalogados internacionalmente mediante el convenio de Ciberdelincuencia[11] y Colombia no ha ratificado su participación activa de este Convenio, aunque se tomó como pilar en la formulación de la Ley 1273 de 2009, no se lo adoptó en su totalidad, por esta causa es necesario volver a retomarlo para actualizar la caracterización de los delitos e identificarlos con el mismo nombre como se conocen a nivel internacional.

La Ley 1273 del 05 de Enero de 2009 de la República de Colombia necesita encontrar un contraste con la legislación afín en países que tienen similares condiciones como: que hablen el mismo idioma, que tengan similitud en la economía, el poder militar, estabilidad, población, desarrollo y el papel en el mundo[12],como Argentina, Costa Rica, Chile, Ecuador, Perú y Venezuela, para crear un ambiente balanceado en el que se pueda establecer una comparación beneficiosa que enriquezca la formulación de las nuevas normas.

[11]Serie de Tratados Europeos-n° 185. *Convenio sobre la Ciberdelincuencia*. Budapest, Concilio de Europa.
[12] Carlos 1234 (2012). *Países más Poderosos de América Latina*. Recuperado de http://listas.20minutos.es/lista/paises-mas-poderosos-de-america-latina-337996/.

Los delitos informáticos son un problema global, traspasan las fronteras, en algunos países estos delitos son tan temidos que se han creado organizaciones especializadas, encargadas de velar por la protección de la información y los datos como es el caso de España con su propia Dirección General de Policía en contra de los ciberdelincuentes, México con su Instituto Federal de Acceso a la información y Protección de Datos, en Estados Unidos el FBI dispone de personal dedicado únicamente a perseguir a los ciberdelincuentes. Y reconociendo que así como crece la población en el ciberespacio, crece la posibilidad de delinquir por este medio, se debe velar más profusamente por establecer barreras que contrarresten estos ataques; por ello es necesario inspeccionar las leyes específicas que combaten contra los delitos específicos que pueden golpear en cualquier momento, no esperar a que ocurra un hecho gravísimo para actuar, sino que teniendo la oportunidad de hacer análisis comparativos no se puede decir que no existen las herramientas para mejorar los planteamientos.

El mismo entorno tecnológico cambiante obliga a los entes legislativos a evaluar su sistema legal, es necesario determinar las falencias existentes en la norma sobre delitos informáticos a la luz de otras legislaciones y de tratados internacionales, que permitan proyectar leyes adecuadas y efectivas que cumplan con su misión de proteger. Y estos entes buscan puntos de vista que favorezcan o amplíen su visión de la problemática, y la buscarán en las fuentes que se especializan en el estudio de estas áreas temáticas, en este caso, entre los estudiosos de los sistemas informáticos, es un deber de los profesionales del área poner a disposición documentos que faciliten esas consultas.

2.2 FORMULACION DEL PROBLEMA

¿Cómo la identificación de las falencias existentes en la Legislación Colombiana sobre Delitos Informáticos ayudará a plantear mejoras en el sistema jurídicode la Ley 1273 de 2009, para la tipificación y tratamiento de estos delitos?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Plantear mejoras para la tipificación y tratamiento de los delitos informáticos mediante un estudio comparativo con otros países que permita identificar las falencias en el sistema jurídico colombiano de la Ley 1273 de 2009.

3.2 OBJETIVOS ESPECIFICOS

- Consultar la normativa vigente sobre Delitos Informáticos en los países de Latinoamérica y seleccionar algunos de los países de acuerdo a criterios y similitudes con la legislación de Colombia.

- Determinar los delitos informáticos y cuáles actividades delictivas se catalogan de acuerdo a la Organización de las Naciones Unidas (ONU) en el Convenio de Ciberdelincuencia de 2001[13] realizado en Budapest.

- Determinar las diferencias y similitudes que existen entre la normatividad Colombiana y las normatividades de los países analizados mediante un análisis comparativo.

- Caracterizar las falencias de la Ley 1273 de 2009 identificadas en el análisis comparativo de las leyes bajo las definiciones planteadas en el Convenio de Ciberdelincuencia[13].

- Plantear mejoras en la legislación nacional respectoal tema de Delitos Informáticos a partir de las falencias identificadas.

[13]Serie de Tratados Europeos-n° 185. *Convenio sobre la Ciberdelincuencia.* Budapest, Concilio de Europa.

4. MARCO TEORICO

4.1 MARCO CONCEPTUAL

4.1.1Delito Informático.

En primer lugar se define el Delito como tal, se acuña la definición de un ilustre en el tema de las ciencias jurídicas:

Ferri: «Son delitos las acciones determinadas por motivos individuales (egoístas) y antisociales, que turban las condiciones de vida y lesionan la moralidad media de un pueblo dado, en un momento dado»[14].

Hace ya algún tiempo se viene operando en el ambiente tecnológico el concepto de Delito informático, muchos organismos han emitido sus conceptos desde diferentes puntos de vista. Muchos consideran que no es necesario hacer la diferencia con los delitos tradicionales, un ejemplo claro de este concepto se demuestra en el Código Penal de España, en el cual no se compendian los Delitos Informáticos en un grupo específico, los artículos que se emplean a la hora de castigar un Delito Informático se encuentran inmersos en distintos lugares de la normatividad española.

Un punto de referencia que puede dar un concepto universal de Delito Informático en un ambiente internacional es el "Convenio de Ciberdelincuencia del Consejo de Europa"[15], del cual se puede decir:

Delitos Informáticos: "los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos"[16].

Este tipo de Delitos tiene las siguientes características:

[14]Monografías. *Definiciones de Delito*. Recuperado de http://www.todoiure.com.ar/monografias/mono/penal/Definiciones_de_delito.htm.
[15]Serie de Tratados Europeos-n° 185. *Convenio sobre la Ciberdelincuencia.* Budapest, Concilio de Europa.
[16] División ComputerForensic, (2012). *Definición de Delito Informático.* Recuperado de http://delitosinformaticos.info/delitos_informaticos/definicion.html.

- “Son delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas.
- Son actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.
- Los **delitos informáticos** tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los mismos”[17].

En definitiva, el Delito Informático es todo acto que haga uso de medios informáticos, que sea contrario a una legislación establecida en un país lo cual acarrea una sanción judicial.

4.1.2Convenio de Ciberdelincuencia De 2001.

El Delito Informático fue tema de discusión hace 13 años, cuando en Budapest se reunieron los Países miembros, hasta ese entonces, de la ONU (Organización de Naciones Unidas) para definir los diferentes delitos informáticos como precedente a lo que sería en adelante la fuente principal para legislar acerca de este tipo de problemática que desde entonces cobraba fuerza en todo el ámbito informático, flagelo que se ha ido extendiendo y desarrollando a la par de los diferentes avances tecnológicos.

Existen fuentes muy importantes que ofrecen la tipología de los Delitos informáticos, pero para el estudio propuesto se toma como base el “Convenio de Ciberdelincuencia”[18] firmado en Budapest, el 23 de noviembre de 2001, el cual entró en vigencia el 01 de Julio de 2004.

Adoptado en la actualidad por 43 países según estadísticas que presenta el Concilio de Europa en su sitio web de seguimiento al Convenio[19].

---

[17] División ComputerForensic, (2012). *Definición de Delito Informático.* Recuperado de http://delitosinformaticos.info/delitos_informaticos/definicion.html.

[18] Serie de Tratados Europeos-n° 185. *Convenio sobre la Ciberdelincuencia.* Budapest, Concilio de Europa.

[19] Council of Europe, (2014).*Convention on Cybercrim CETS No.: 185.*Recuperado de http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG.

Siendo uno de los últimos países no miembros Panamá, quien Ratificó su posición frente al convenio el 5 de Marzo de 2014, y entró en vigencia a partir del primero de Julio de 2014. Y de los países miembros el último a la fecha en Ratificar su adhesión al Convenio es Turquía el 29 de Septiembre de 2014 para entrar en vigencia a partir del Primero de Enero de 2015.

Colombia no ha ratificado su adhesión al Convenio pero se encuentra en el listado de países que han declarado su interés y aprobación del mismo.

El Convenio de Ciberdelincuencia define los Delitos Informáticos distribuidos en cuatro (4) grupos, así:

1. 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: Interferencia en los datos (Ataques a la integridad de los datos)
   Art. 5: Interferencia en el sistema (Ataques a la integridad del sistema)
   Art. 6: Abuso de los dispositivos

2. Delitos informáticos.
   Art. 7: Falsificación informática
   Art. 8: Fraude informático

3. Delitos relacionados con el contenido.
   Art. 9: Delitos informáticos relacionados con la pornografía infantil

4. 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.

Para el presente estudio se han seleccionado 8 de los 10 Artículos del Convenio Ciberdelincuencia, el Artículo 1 no se menciona porque en este hace referencia a un glosario de términos, y el Artículo 10 no se incluye en el estudio porque abarcaría un análisis más extenso que incluiría la mención de otras leyes que protegen a los ciudadanos de delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines; los siguientes Artículos se tienen en cuenta en el análisis comparativo:

Artículo 2: Acceso ilícito: "Acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático**"**[20].

Artículo 3: Interceptación ilícita: "la interceptación deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático**"**[20]

Artículo 4: Interferencia en los datos: "la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos"[21].

Artículo 5:Interferencia en el sistema: "la obstaculización grave, deliberada eilegítima del funcionamiento de un sistema informático mediante la introducción,transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datosinformáticos.**"**[21]

Artículo 6: Abuso de los dispositivos: "La comisión deliberada e ilegítima de … la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículos 2 a 5; una contraseña, un código de acceso o datos informáticos similares que permitan tener acceso a la totalidad o a una parte de un sistema informático". "La posesión de alguno de los elementos contemplados", "con el fin de cometer cualquiera de los delitos previstos en los artículos del 2 al 5**"**[21].

Artículo 7: Falsificación Informática: "cuando se cometa de forma deliberada eilegítima, la introducción, alteración, borrado o supresión de datos informáticos que délugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizadosa efectos legales como si se tratara de datos auténticos, con independencia de que losdatos sean o no directamente legibles e inteligibles. Cualquier Parte podrá exigir queexista una intención fraudulenta o una intención delictiva similar para que se considereque existe responsabilidad penal**"**[21]

[20]Serie de Tratados Europeos-n° 185. *Convenio sobre la Ciberdelincuencia.* Budapest, Concilio de Europa.
[21]Serie de Tratados Europeos-n° 185. *Convenio sobre la Ciberdelincuencia.* Budapest, Concilio de Europa.

Artículo 8: Fraude Informático: "los actos deliberados e ilegítimos quecausen un perjuicio patrimonial a otra persona mediante:
a) Cualquier introducción, alteración, borrado o supresión de datos informáticos;
b) Cualquier interferencia en el funcionamiento de un sistema informático,con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficioeconómico para uno mismo o para otra persona**"**[21]

Artículo 9: Delitos relacionados con la Pornografía Infantil: Todo lo relacionado a la Producción de Pornografía Infantil, oferta, difusión o transmisión, adquisición, posesión, utilizando sistemas informáticos.

Según referencia del Doctor Santiago Acurio del Pino (Profesor de Derecho Informático) a través de su libro "Delitos Informáticos: Generalidades", en la página 49, manifiesta que La INTERPOL en su 6ª Conferencia Internacional sobreCiberdelincuencia realizada en el Cairo (Egipto), del 13 al 15 de abril de 2005, recomienda a todos los países miembros de la INTERPOL (que actualmente opera en 190 países), que se utilice el Convenio de Ciberdelincuencia del Consejo de Europa como fuente para legislar en materia de Delitos Informáticos.[22]

Del Artículo 9 se hace referencia en la primera parte del estudio, lo referente a la existencia o no de leyes que atiendan esta clase de delito, lo cual está bien contemplado en la legislación Colombiana en la Ley 1336 de 2009 que se emitió para robustecer la Ley 679 de 2001 sobre la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes.

Acurio también recalca en sus libros considerar la cooperación Internacional en lo referente al cibercrimen porque es un fenómeno que traspasa fronteras y a todos atañe.

4.2 MARCO LEGAL

4.2.1 El Sistema del Derecho Romano. Este sistema tiene origen en el continente Europeo, su nombre es tomado de la antigua Roma que fue la cuna del derecho

[22]Acurio, S. *Delitos Informáticos*: *Generalidades.* Quito – Ecuador. Pontificia Universidad Católica del Ecuador (PUCE).

escrito o codificado en lo que hoy se conoce como Constitución Política de un país, es el compendio de diferentes normas las cuales rigen sobre una nación.

4.2.2 El Sistema del Derecho Anglosajón o "CommonLaw". Este sistema nace en el continente norteamericano, se caracteriza por tener pocas leyes escritas, su fuente principal es el conjunto de sentencias o lo que se conoce como jurisprudencia, de modo que los fallos determinados en un juicio son aplicados conforme a lo que se ha fallado en casos similares, buscando aplicar la justicia de acuerdo a los acontecimientos comunes que han sucedido.

Partiendo de estas cortas definiciones se direcciona el estudio unificando conceptos, es decir, se estudiará la legislación Colombiana la cual se fundamenta en El Sistema del Derecho Romano determinando países que se encuentren bajo la misma condición.

4.2.3 Descripciónde las Legislaciones sobre Delitos Informáticos: Estudiando las diversas legislaciones que pueden ser utilizadas para castigar el delito informático, a nivel internacional se ha tomado como referencia las leyes descritas a continuación:

Legislación Delitos Informáticos en Colombia:

El 5 de enero de 2009, el Congreso de la República promulgó la "Ley 1273", la cual modificó el código penal adicionando nuevas sanciones en casos relacionados con los delitos informáticos, buscando proteger la información y preservar los sistemas de tecnologías de información y comunicaciones. Esta ley contempla dos capítulos: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos", y "De los atentados informáticos y otras infracciones".[23]

Legislación Delitos Informáticos en Argentina:

En Argentina, en Junio del 2008 se promulgó la "Ley No 26388" (56) con reformas al Código Penal modificando delitos existentes e incluyendo el alcance de los términos documento, firma, suscripción, instrumento privado y certificado, y de esta manera contemplar el uso de nuevas tecnologías. Esta reforma contempló los siguientes delitos: La pornografía infantil mediante el uso de internet u otros medios digitales, el robo y acceso no autorizado de información almacenada

[23]Calderón R, Guzmán G, Salinas J. (2011). *Diseño y Plan de Implementación de un Laboratorio de Ciencias Forenses Digitales Tesina de Seminario.* Guayaquil – Ecuador. Escuela Superior Politécnica del Litoral.

digitalmente, fraude y sabotaje informático, interferencias en comunicaciones, entre otros.[24]

Legislación Delitos Informáticos en Costa Rica:

La presidenta Laura Chinchilla firmó la Ley 9048 "Reforma de varios artículos y modificación de la sección VIII denominada delitos informáticos y conexos, del título VII del Código Penal".

Esta ley sanciona el delito de corrupción, también contempla la violación de correspondencia o comunicaciones, violación de datos personales, extorsión, estafa informática, daño informático, espionaje, sabotaje informático, suplantación de identidad, espionaje informático, instalación o propagación de programas informáticos maliciosos, suplantación de páginas electrónicas, facilitación de delito informático y difusión de información falsa.

Legislación Delitos Informáticos en Chile:

Fue el primer país latinoamericano en expedir una "Ley contra los delitos informáticos", Ley19223del 28 de Mayo de 1993, la cual consta de cuatro artículos en los que se castigó conductas ilícitas como: la inutilización o destrucción de un sistema de tratamiento de información o sus componentes afectando el correcto funcionamiento del sistema, al igual que la interferencia, intercepción o acceso a un sistema de información con el fin de apoderarse de datos almacenados en el mismo, también sancionó el daño o destrucción de datos, así como la revelación o difusión de datos contenidos en un sistema de una manera malintencionada.[25]

Legislación Delitos Informáticos en Ecuador:

"Dentro del nuevo Código Penal del Ecuador ya se especifican varios tipo de delitos informáticos. Los artículos que los tipifican son el 229 y el 234. Se toman en cuenta delitos por revelación ilegal de base de datos, transferencia electrónica por activo patrimonial, intercepción ilegal de datos, ataque a la integridad de sistemas informáticos, delitos contra la información pública reservada, y acceso no consentido a un sistema informático."[26]

---

[24]Calderón R, Guzmán G, Salinas J. (2011). *Diseño y Plan de Implementación de un Laboratorio de Ciencias Forenses Digitales Tesina de Seminario.* Guayaquil – Ecuador. Escuela Superior Politécnica del Litoral.

[25]Calderón R, Guzmán G, Salinas J. (2011). *Diseño y Plan de Implementación de un Laboratorio de Ciencias Forenses Digitales Tesina de Seminario.* Guayaquil – Ecuador. Escuela Superior Politécnica del Litoral.

[26]Ecuador. (06 de Enero de 2014). Se tipifican los delitos informáticos en el nuevo Código Penal del Ecuador. *Movistar*. Recuperado de http://www.movistar.com.ec/comunidad/showthread.php?514-Se-tipifican-los-delitos-inform%E1ticos-en-el-nuevo-C%F3digo-Penal-del-Ecuador.

Legislación Delitos Informáticos en Perú:

La ley peruana sobre delitos informáticos fue sancionada el 26 de Junio del 2000, la Ley 27309 sancionó a los que utilizan o ingresan indebidamente a un sistema informático, a quien interfiere indebidamente una base de datos o sistema informático; esta Ley fue actualizada mediante la Ley 30096 del 27 de septiembre de 2013, modificada mediante la Ley 30171 del 17 de Febrero de 2014, en la cual se incluyeron los delitos de acceso ilícito, atentado contra la integridad de datos y sistemas informáticos, sanciona los delitos informáticos contra la indemnidad y libertad sexuales, tráfico ilegal de datos, interceptación de datos informáticos, fraude informático, suplantación de identidad, abuso de mecanismos y dispositivos informáticos.

Esta legislación es una de las más completas porque contempla muy claramente todos los delitos que se establecen en el Convenio de Ciberdelincuencia de 2001[27] y en sus disposiciones finales promueve la firma y ratificación de Convenios multilaterales que garanticen la cooperación mutua con otros países para la persecución de delitos informáticos[28]

Legislación Delitos Informáticos en Venezuela:

El país Bolivariano sancionó una ley especial sobre Delitos Informáticos, compuesta por 33 artículos clasificados en 5 Capítulos entre los temas que abarca se encuentran artículos contra sistemas que utilizan TI, la propiedad, la privacidad de las personas y las comunicaciones; para la protección de los niños y adolescentes y el orden económico[29].

4.3 MARCO CONTEXTUAL

En Colombia el delito informático se sanciona mediante la Ley 1273 del 05 de enero de 2009 denominada “de la protección de la información y de los datos”, en ella se contemplan 10 delitos sancionados que son:

Artículo 269A: Acceso abusivo a un sistema informático. En el cual se castiga al que sin estar autorizado o la fuerza acceda a un sistema informático.

[27]Serie de Tratados Europeos-n° 185. *Convenio sobre la Ciberdelincuencia*. Budapest, Concilio de Europa.
[28] Normas Legales – El Peruano. (2014). *Ley No. 30171 – Ley que Modifica La Ley 30096*, Ley de Delitos Informáticos. Perú. Congreso de la República
[29]Temperini, Marcelo Gabriel Ignacio. (2013). *Delitos Informáticos en Latinoamérica: Un estudio comparado. 1ra. Parte.* Argentina. Universidad Nacional del Litoral.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación: Sanciona al que impide el funcionamiento normal de un sistema informático, o impide el acceso normal a una red de telecomunicación.

Artículo 269C: Interceptación de datos informáticos. Se sanciona a aquel que intercepta datos informáticos sin tener una orden judicial para ello.

Artículo 269D: Daño Informático. Se castiga al que destruye, daña, borra, deteriora, altera o suprime datos informáticos sin estar autorizado para ello.

Artículo 269E: Uso de software malicioso. Sanciona al que trafica, produce, distribuye o vende programas maliciosos o software con efectos dañinos.

Artículo 269F: Violación de datos personales. Se penaliza al que obteniendo datos personales o información privada de un tercero los emplea para su propio provecho.

Artículo 269G: Suplantación de sitios web para capturar datos personales. Sanciona al que usa páginas electrónicas, enlaces o ventanas emergentes falsas para obtener datos confidenciales que usará para su beneficio.

Artículo 269H: Circunstancias de agravación punitiva. Describe los agravantes de las penas sí el delito se comete en redes o sistemas de organismos públicos, o en el sector financiero, sí es funcionario público, o contratistas que trabajan en el medio estatal, quien hace daño a un tercero revelando información confidencial, quien actúa con fines terroristas, se sanciona al administrador de sistemas de información que obra de mala fe con inhabilidad en sus funciones.

Artículo 269I: Hurto por medios informáticos y semejantes. Se castiga al que por medio de sistemas informáticos hurta, o suplanta a un usuario ante los sistemas de autenticación.

Artículo 269J: Transferencia no consentida de activos. Se sanciona al que manipulando un sistema transfiere activos perjudicando a un tercero, y lo hace para su propio lucro. Y también se sanciona al que fabrica, provee o facilita software que se utilice para realizar este tipo de delito.

5. ASPECTOS METODOLÓGICOS

5.1 TIPO DE INVESTIGACIÓN

La Investigación es de tipo bibliográfico, cualitativa de tipo evaluativa por cuanto se estudia la normativa en cuanto a delitos informáticos en los seis países seleccionados para definir las falencias que existen en la legislación colombiana.

5.2 POBLACIÓN

La población está constituida por la legislación sobre delitos informáticos en 35 países de Latinoamérica[30]:

1 ARGENTINA
2 BAHAMAS
3 BARBADOS
4 BELICE
5 BERMUDAS
6 BOLIVIA
7 BRASIL
8 CHILE
9 COLOMBIA
10 COSTA RICA
11 CUBA
12 DOMINICA
13 ECUADOR
14 EL SALVADOR
15 GRANADA
16 GUATEMALA
17 GUYANA
18 HAITÍ
19 HONDURAS
20 ISLAS CAIMÁN (GB)
21 JAMAICA
22 MÉXICO
23 MONTSERRAT
24 NICARAGUA
25 PANAMÁ
26 PARAGUAS
27 PERÚ
28 PUERTO RICO
29 REPÚBLICA DOMINICANA
30 SAN VICENTE Y LAS GRANADINAS
31 SANTA LUCÍA
32 SURINAME (PAISES BAJOS)
33 TRINIDAD Y TOBAGO
34 URUGUAY
35 VENEZUELA

5.3 MUESTRA

Esta muestra es de carácter representativo, que está constituida por la legislación sobre delitos informáticos de seis países de Latinoaméricafuera de Colombia, que son:Argentina,Costa Rica, Chile, Ecuador,Perú y Venezuela.

[30] Depósito de documentos de la FAO. (2013). *América Latina y El Caribe.* Recuperado de: http://www.fao.org/docrep/v8300s/v8300s0o.htm.

5.4 VARIABLES

La legislación sobre delitos informáticos de los países seleccionados:

Colombia: Ley 1273 del 05 de Enero de 2009 (Ver ANEXO A), Ley 1336 de 2009 (Ver ANEXO B)

Argentina: Ley 25326 del 30 de Octubre de 2000 (Ver ANEXO C), Ley 26388 del 24 de Junio de 2008 (Ver ANEXO D).

Costa Rica: Ley 9048 de 2012 (Ver ANEXO E)

Chile: Ley 19223 del 28 de Mayo de 1993 (Ver ANEXO F) y Ley No. 19.927, del 05 de enero de 2004 (Ver ANEXO G)

Ecuador: Ley 67 del 27 de Febrero de 2002 (Ver ANEXO H)

Perú: Ley No. 30096 del 22 de Octubre de 2013 (Ver ANEXO I) y la Ley 30171 del 06 de Marzo de 2014 (Ver ANEXO J).

Venezuela: Ley Especial Contra los Delitos Informáticos del 04 de Septiembre de 2001(Ver ANEXO K).

6. DESARROLLO DEL ESTUDIO COMPARATIVO

6.1METODOLOGIA DE DESARROLLO DEL ESTUDIO COMPARATIVO

Para lograr los objetivos propuestos fue necesario utilizar la siguiente metodología:

1. Se determinó utilizar un lineamiento internacional que permita la tipificación clara de los delitos Informáticos, para establecer un parámetro que apoye la identificación de este tipo de delitos dentro de la legislación de los países seleccionados.

2. Se Identificó el estado del arte del trato legislativo sobre los delitos informáticos en la normativa internacional, esto se consiguió consultando diferentes fuentes en internet, se analizaron los delitos dentro de la legislación de cada país, se obtuvo información de estudios críticos de esas legislaciones, se tuvieron en cuenta los proyectos de ley de delitos informáticos para conocer la exposición de motivos y las bases teóricas sobre las cuales se propuso la tipificación de los delitos informáticos. A partir de este análisis se eligió la normativa de 6 países de Latinoamérica para comparar con la legislaciónColombiana.

3. Se realizó la comparación de los delitos informáticos con la normatividad de cada país seleccionado para el estudio, teniendo en cuenta las definiciones de los delitos catalogados en el Convenio de Ciberdelincuencia [31] y determinando sí sobre cada delito existe legislación específica para su sanción. En la revisión de las definiciones se tiene en cuenta sí se utilizan los términos sugeridos en el Convenio, y especialmente se hace énfasis en el título con que se refiere el delito, buscando cada artículo en el que predomine la caracterización determinada por la ONU, y estos artículos son los seleccionados para exponer como resultado en el cuadro comparativo.

4. También se realizó la comparación de los delitos informáticos sancionados en la legislación colombiana (Ley 1273 de 2009) con los similares de las legislaciones de los países objeto del estudio, teniendo en cuenta el título del delito y su definición para determinar el grado de aproximación en la tipificación, esto permite conocer sí un delito en Colombia se conoce de la misma forma en otros países que hablan el mismo idioma.

5. Se identificaron las fortalezas y debilidades existentes en la normativa colombiana sobre delitos informáticos como resultado de la comparación

[31]Serie de Tratados Europeos-n° 185. *Convenio sobre la Ciberdelincuencia.* Budapest, Concilio de Europa.

con las leyes sobre el mismo tema en los países seleccionados para el estudio; este ejercicio permite poner en balanza el contenido de cada artículo de la Ley 1273 de 2009, de lo cual es más fácil denotar las diferencias y catalogarlas como puntos fuertes o puntos débiles.

6. En base a las debilidades encontradas se identificaron las falencias existentes en la legislación Colombiana sobre delitos informáticos, resultantes delanálisis comparativo con la definición del trato jurídico al respecto en los países seleccionados. Estos faltantes se pueden contrastar al mismo tiempo con la recomendación de mejora de cada uno, enfocados en la visión de plantear soluciones que lleven a la tipificación del delito a un nuevo nivel, un alto nivel en el que pueda ser definido en un lenguaje comprensible y con carácter global; esto permiteestablecer un marco para los delitos futuros.

7. Como resultado de la investigación bibliográfica se planteó un cuadro de mejoras a la Ley 1273 de 2009, en el cual se realizan recomendaciones basadas enlas falencias identificadas, se tomaron apartes de algunos artículos de las legislaciones de los países seleccionados que pueden enriquecer la normativa colombiana, y se presenta en relieve alternativasmás clarasde cómo tipificar estos delitos, teniendo siempre como lineamiento las definiciones de delitos informáticos que ofrece el Convenio de Ciberdelincuencia[32].

Mediante este tipo de estudio se evalúa la posición que ha tomado Colombia frente a la problemática de los Ciberdelincuentes.Para una mayor comprensión fue necesario establecer una base temática que permita delimitar el tema a tratar de la siguiente forma:

- Entre la infinidad de delitos que atentan contra la integridad de los datos, para el presente estudio de análisis comparativo se tendrá en cuenta los delitos de mayor importancia consignados en el Convenio de Ciberdelincuencia[32]: Acceso ilícito, Interceptación ilícita, Ataques a la integridad de los datos, Ataques a la integridad del sistema, Abuso de los dispositivos, Falsificación Informática, Fraude Informático, Delitos relacionados con la Pornografía Infantil.

[32]Serie de Tratados Europeos-n° 185. *Convenio sobre la Ciberdelincuencia.* Budapest, Concilio de Europa.

- Se realiza el análisis centrado en el contenido de la Ley 1273 del 05 de Enero de 2009 de la República de Colombia, con sus afines en la legislación del mismo tema jurídico en los países de Argentina, Costa Rica, Chile, Ecuador, Perú y Venezuela.

A continuación se muestran los criterios utilizados para la selección de los países sobre los cuales se realiza el estudio:

- Se eligieron 6 países además de Colombia para obtener un total de 7 países como representación de la quinta parte de la población total de 35 países de Latinoamérica, teniendo en cuenta la información que ofrecen en cuanto a su regulación en el tema de los Delitos Informáticos.

- Se tomaron los seis países de acuerdo, la economía, el poder militar, estabilidad, población, desarrollo y su papel en el mundo. [33]

- Los países elegidos hablan el mismo idioma.

- Los países seleccionados tienen legislación específica sobre Delitos Informáticos.

- Los artículos que se tomaron como objeto de estudio de cada país, están directamente relacionados con la definición sobre delitos informáticos catalogados según el Convenio de Ciberdelincuencia de 2001[34].

- Los países seleccionados han manifestado estar de acuerdo con los conceptos emitidos por la ONU en cuanto a delitos informáticos

Siguiendo con el desarrollo del estudio, se presenta las comparaciones propuestas en el Objetivo General. Se determinaron los delitos informáticos catalogados por la ONU en el Convenio de Ciberdelincuencia[34]:Acceso ilícito, Interceptación ilícita, Ataques a la integridad de los datos, Ataques a la integridad del sistema, Abuso de los dispositivos, Falsificación Informática, Fraude Informático, Delitos relacionados con la Pornografía Infantil.

Teniendo en cuenta este dato, se realizaron diferentes cuadros comparativos con los cuales se somete la Legislación colombiana a cotejo; los cuadros realizados

[33] Carlos 1234 (2012). *Países más Poderosos de América Latina*. Recuperado de http://listas.20minutos.es/lista/paises-mas-poderosos-de-america-latina-337996/.
[34] Serie de Tratados Europeos-n° 185. *Convenio sobre la Ciberdelincuencia.* Budapest, Concilio de Europa.

ofrecen la posibilidad de analizar sus artículos detenidamente, por ejemplo, en el Cuadro 1 se obtiene la Legislación por cada delito informático reconocido a nivel internacional, respecto a cada uno de los países objeto de estudio, lo cual brinda una clara visualización de la posición que tiene Colombia frente a estos delitos; en seguida, en el Cuadro 2 se realiza el cruce de información para determinar las sanciones por cada delito informático seleccionado en cada país, de este ejercicio se obtienen más puntos de referencia para establecer criterios que permiten plantear mejoras.

En el Cuadro 3 se realiza un análisis directo sobre la Ley 1273 de 2009, cotejando cada artículo con los que tratan el mismo tema jurídico de los 6 países seleccionados, para determinar algunos faltantes importantes en esta Ley que se estarán sintetizando en el capítulo 7.

6.2LEGISLACIÓN SOBRE DELITOS INFORMATICOS

En el Cuadro 1 se identifica los delitos catalogados según el Convenio de Ciberdelincuencia de Budapest[35], en comparación con los países objetos del estudio, en primer lugar se encuentra Colombia, seguidos de los seis países seleccionados: Argentina, Costa Rica, Chile, Ecuador, Perú y Venezuela, donde se determina si en la legislación de cada país se reglamentan los ocho (8) delitos informáticos según este Convenio:

1. Acceso ilícito,
2. Interceptación ilícita,
3. Ataques a la integridad de los datos,
4. Ataques a la integridad del sistema,
5. Abuso de los dispositivos,
6. Falsificación Informática,
7. Fraude Informático,
8. Delitos relacionados con la Pornografía Infantil.

Se aclara que el tercer delito de Ataques a la integridad de los datos en el convenio se identifica como “Interferencia en los datos” y el cuarto delito de

[35]Serie de Tratados Europeos-n° 185. *Convenio sobre la Ciberdelincuencia.* Budapest, Concilio de Europa.

Ataques a la integridad del sistema se denomina “Interferencia en el sistema”, se conserva esta modificación en el cuadro 1 reconociendo los derechos de autor.

Cuadro1.Cuadro de Derecho Comparado clasificado de acuerdo a los delitos informáticos

PAIS	Acceso Ilícito	Intercepta ción Ilícita	Ataques a la Integrida d de los datos	Ataques a la Integrida d del Sistema	Abuso de los dispositivos	Falsificación Informática	Fraude Informátic o	Pornografí a Infantil
Colombia	Ley 1273 Art. 269A	Ley 1273 Art. 269C	Ley 1273 Art. 269D y F	Ley 1273 Art. 269B y D	No encontrado.	No encontrado.	Ley 1273 Art. 269J	Ley 1336 Art. 24
Argentina	Art. 153 bis	Art. 153	Art. 183 2do párrafo	Art. 183 2do Párrafo y Art. 197.	No encontrado.	Art. 292	Art. 173 Inc. 16	Art. 128
Costa Rica	Art. 196	Art. 196	229 bis	Art. 229 ter	No encontrado.	217 bis	217 bis	Art. 167
Chile	Art.2	Art.2	Art. 3	Art. 1	No encontrado.	No encontrado.	No encontrado.	Art. 374 bis CP
Ecuador	Art. 202.1	No encontra-do.	Art. 415.1	No encontra-do.	No encontrado	Art. 353.1	Art. 563 Inc. 2	Art. 528.7 Código penal
Perú	LEY Nº 30096 Art. 2	Art.7	Art. 3	Art. 4	Art. 10 .	No encontrado.	Art. 8 .	Ley 28.251 – Art. 183 A
Venezuel a	Art. 6	Art. 21	Art. 7 2do párrafo	Art. 7. 1er párrafo	Art. 10 y 19	Art. 12	Art. 14	Art. 24

Fuente: Marcelo Gabriel Ignacio[36]

Partiendo del concepto de tipificación legal que significa dar un nombre al acto que está afectando un bien jurídico, al hecho que se está considerando como ilícito; en este caso el derecho penal es un sistema cerrado que no permite la analogía[37] o interpretación de la ley, que trate de ajustar los contenidos hacia delitos castigados por la norma. Se puede concluir que los faltantes que demuestra el Cuadro 1 son relevantes y posteriormente se exponen en el Análisis, numeral 7.1.

[36] Temperini, Marcelo Gabriel Ignacio. *Delitos Informáticos en Latinoamérica: Un estudio de derecho comparado. 1ra. Parte.* Argentina, Universidad Nacional del Litoral.

[37] El Derecho en su interpretación Judicial. (2008). *Prohibición de la aplicación de la Analogía.* Jurisprudencia Penal.

6.3 SANCIONES LEGISLADAS POR CADA DELITO

Del Cuadro 1 se puede extender la apreciación al campo de las sanciones impuestas por cada delito catalogado por la ONU y especificando las sanciones que tiene cada delito; el Cuadro 2 permite determinar otro punto de comparación, donde se aprecia el rigor ejercido en los castigos legislados en cada país:

Cuadro 2. Sanciones por Delito

PAIS	DELITO	SANCION
Colombia	Acceso Ilícito	Prisión de 48 a 96 meses y multa de 100 a 1.000 Salarios Mínimos Legales Mensuales Vigentes.
	Interceptación Ilícita	Prisión de 36 a 72 meses
	Ataques a la Integridad de los datos	Prisión de 48 a 96 meses y multa de 100 a 1.000 Salarios Mínimos Legales Mensuales Vigentes.
	Ataques a la Integridad del Sistema	Prisión de 48 a 96 meses y multa de 100 a 1.000 Salarios Mínimos Legales Mensuales Vigentes por Obstaculización ilegítima del sistema Informático o redes de telecomunicación, y Prisión de 48 a 96 meses y multa de 100 a 1.000 Salarios Mínimos Legales Mensuales Vigentes por Daño Informático.
	Abuso de los dispositivos	No contemplado
	Falsificación Informática	No contemplado
	Fraude Informático	Prisión de 48 a 120 meses y multa de 200 a 1.500 Salarios Mínimos Legales Mensuales Vigentes.
	Pornografía Infantil	Prisión de 10 a 20 años y multa de 150 a 1.500 salarios mínimos legales mensuales vigentes
Argentina	Acceso Ilícito	Prisión de quince (15) días a seis (6) meses
	Interceptación Ilícita	Prisión de quince (15) días a seis (6) meses
	Ataques a la Integridad de los datos	Prisión de quince días a un año
	Ataques a la Integridad del Sistema	Prisión de quince días a un año, por interceptar telecomunicaciones prisión de seis (6) meses a dos (2) años
	Abuso de los dispositivos	No contemplado
	Falsificación Informática	Prisión de uno a seis años, si se tratare de un instrumento público y con prisión de seis meses a dos años, si se tratare de un instrumento privado
	Fraude Informático	Prisión de un mes a seis años
	Pornografía Infantil	Prisión de seis meses a cuatro años
Costa Rica	Acceso Ilícito	Prisión de tres a seis años, y por agravantes puede ir hasta de cuatro ocho años.
	Interceptación Ilícita	Prisión de tres a seis años, y por agravantes puede ir hasta de cuatro ocho años.
	Ataques a la Integridad de los datos	Prisión de uno a tres años, por agravantes la pena de prisión de tres a seis años
	Ataques a la Integridad del Sistema	Prisión de uno a tres años, por agravantes la pena de prisión de tres a seis años

Cuadro 2. (Continuación)

	Abuso de los dispositivos	No contemplado
	Falsificación Informática	Prisión de tres a seis años, por agravantes serán cinco a diez años de prisión
	Fraude Informático	Prisión de tres a seis años, por agravantes serán cinco a diez años de prisión
	Pornografía Infantil	Prisión de tres a ocho años, por agravantes serán cuatro a diez años de prisión
Chile	Acceso Ilícito	Prisión menor en su grado mínimo a medio. De 61 días a 3 años.
	Interceptación Ilícita	Prisión menor en su grado mínimo a medio. De 61 días a 3 años.
	Ataques a la Integridad de los datos	Prisión menor en su grado medio. De 2 años y un día a 3 años.
	Ataques a la Integridad del Sistema	Prisión menor en su grado medio a máximo. De 2 años y un día a 5 años.
	Abuso de los dispositivos	No contemplado
	Falsificación Informática	No contemplado
	Fraude Informático	No contemplado
	Pornografía Infantil	Para quien lo produce Prisión menor en su grado medio a máximo, de 2 años y un día a 5 años. Y para quien lo distribuye Prisión menor en su grado medio, de 2 años y un día a 3 años.
Ecuador	Acceso Ilícito	Prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica
	Interceptación Ilícita	No contemplado
	Ataques a la Integridad de los datos	Prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.
	Ataques a la Integridad del Sistema	No contemplado
	Abuso de los dispositivos	No contemplado
	Falsificación Informática	Prisión de dos meses a dos años y multa de mil a dos mildólares de los Estados Unidos de Norteamérica.".
	Fraude Informático	uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica
	Pornografía Infantil	pena de dieciséis o veinticinco años de reclusión mayor extraordinaria
Perú	Acceso Ilícito	Pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.
	Interceptación Ilícita	La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.
	Ataques a la Integridad de los datos	Pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

Cuadro 2. (Continuación)

	Ataques a la Integridad del Sistema	Pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.
	Abuso de los dispositivos	Pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.
	Falsificación Informática	No contemplado
	Fraude Informático	Pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.
	Pornografía Infantil	Pena privativa de libertad será no menor de doce ni mayor de quince años.
Venezuela	Acceso Ilícito	Prisión de uno a cinco años y multa de diez a cincuenta unidades tributarias.
	Interceptación Ilícita	Prisión de dos a seis años y multa de doscientas a seiscientas unidades tributarias.
	Ataques a la Integridad de los datos	La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias
	Ataques a la Integridad del Sistema	La pena será de cinco a diez años de prisión y multa de quinientas a mil unidades tributarias
	Abuso de los dispositivos	Prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.
	Falsificación Informática	Prisión de tres a seis años y multa de trescientas a seiscientas unidades tributarias.
	Fraude Informático	Prisión de tres a siete años y multa de trescientas a setecientas unidades tributarias.
	Pornografía Infantil	Prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas unidades tributarias.

Fuente: Los Autores

6.4 CUADRO COMPARATIVO LEY COLOMBIANA VS. LEGISLACIÓN 6 PAISES DE LATINOAMÉRICA

En el Cuadro 3 se realiza un análisis directo sobre cada artículo de la Ley Colombiana No. 1273 de 2009, confrontándola con los artículos que contemplan el mismo tipo de delito en los 6 países seleccionados, este ejercicio permite determinar las fortalezas de la misma.

Cuadro 3. Ley Colombiana vs Legislación de 6 países de Latinoamérica

COLOMBIA	ARGENTINA	COSTA RICA	CHILE	ECUADOR	PERU	VENEZUELA
Ley 1273 "De la Protección de la información y de los datos", del 05/01/09	**La Ley 25.326, de Protección de Datos Personales del 30 de Octubre del 2000**	**Delitos Informáticos y Conexos, del Título VII del Código Penal N° 9048 de 2012**	**Ley relativa a Delitos Informáticos Ley No.:19223 del 7 de Junio de 1993**	**Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos No. 67 del 27/02/2002**	**LEY DE DELITOS INFORMÁTICOS LEY Nº 30096 del 22 de Octubre de 2013**	**Ley Especial Contra los Delitos Informáticos del 30 de Octubre de 2002**
ARTÍCULO 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.	ARTICULO 157 BIS: Violación de Sistemas de confidencialidad y seguridad de datos	ARTICULO 196: Violación de correspondencia o comunicaciones	ARTÍCULO 3: El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento informático.	ARTICULO 5: Confidencialidad y Reserva: Se establecen los principios de confidencialidad y reserva para los mensajes de datos	ARTICULO 2: Acceso ilícito El que accede sin autorización a todo o parte de un sistema informático	ARTÍCULO 6: Acceso indebido. El que sin la debida autorización o excediendo la que hubiere obtenido, acceda, intercepte, interfiera o use un sistema
ARTICULO 269B: OBSTACULIZACIÓN ILEGITIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.	ARTÍCULO 197: El que interrumpe o entorpeciere la comunicación telegráfica, telefónica o de otra naturaleza.			ARTICULO 8: Conservación de los mensajes de datos: Toda información sometida a esta Ley	ARTICULO 4: Atentado contra la integridad de sistemas informáticos, inutiliza, total o parcialmente, un sistema informático, impide el acceso	ARTICULO 12: Falsificación de documentos

Cuadro 3. (Continuación)

ARTICULO 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS.	ARTICULO 128: "Violación de Secretos y de la Privacidad" ARTICULO 153: Acceder indebidamente a una comunicación electrónica para apoderarse de información	ARTICULO 196: Violación de correspondencia o comunicaciones. ARTICULO 229 TER: Sabotaje Informático	ARTICULO 2: El que con ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema…, lo intercepte, interfiera o acceda a el.	ARTICULO 58: Obtención y utilización no autorizada de información	ARTICULO 7: Interceptación de datos informáticos a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas	ARTICULO 19: Posesión de equipo para falsificaciones. El que sin estar debidamente autorizado para emitir, fabricar o distribuir tarjetas inteligentes o instrumentos análogos
ARTÍCULO 269D: DAÑO INFORMÁTICO.	ARTICULO 173 – Inciso 16: …el que manipula o altera un sistema informático	ARTICULO 229 BIS: Daño Informático	ARTICULO 1: El que maliciosamente destruya o inutilice un sistema de tratamiento de información	ARTICULO 61: A Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe	ARTICULO 3: Atentado contra la integridad de datos informáticos borra, deteriora, altera, suprime o hace inaccesibles datos informáticos	ARTICULO 7: Sabotaje o daño a sistemas. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema
ARTÍCULO 269E: USO DE SOFTWARE MALICIOSO.	ARTÍCULO 183: El que altere, destruya o inutilizare datos o doc. … o introdujere un programa dañino.	ARTICULO 232: Instalación o propagación de programas informáticos maliciosos		ARTICULO 57: Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo		
ARTICULO 269F: VIOLACIÓN DE DATOS PERSONALES.	ARTICULO 157 BIS: Violación de … Banco de datos personales	ARTICULO 196 BIS: Violación de datos personales	ARTICULO 4.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información	ARTICULO 9: Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente	ARTICULO 6: Tráfico ilegal de datos El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica	ARTICULO 20: Violación de la privacidad de la data o información de carácter personal

Cuadro 3. (Continuación)

ARTICULO 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES		ARTICULO 233: Suplantación de páginas electrónicas. ARTICULO 217 BIS: Estafa Informática			ARTICULO 9. Suplantación de identidad	
ARTÍCULO 269H: CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA.	ARTICULO 177: Sanciones penales y agravantes.	ARTICULO 229; Daño agravado.				ARTICULO 11: Espionaje informático. El que indebidamente obtenga, revele o difunda la data o información contenidas en un
ARTÍCULO 2691: HURTO POR MEDIOS INFORMÁTICOS y SEMEJANTES.				ARTICULO 60: A Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien	ARTICULO 8: Fraude informático, procura para sí o para otro un provecho ilícito en perjuicio de tercero	ARTÍCULO 13: Hurto. El que a través del uso de tecnologías de información, acceda, intercepte, interfiera, manipule o use de cualquier forma un sistema
ARTÍCULO 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.				ARTICULO 62: A Apropiación ilícita.	ARTICULO 10: Abuso de mecanismos y dispositivos informáticos	ARTICULO 9: Acceso indebido o sabotaje a sistemas protegidos

Fuente: Los Autores

7. ANALISIS DE RESULTADOS

7.1 FALENCIAS RESPECTO AL CONVENIO DE CIBERDELINCUENCIA

Del cuadro 1 se puede determinar claramente las siguientes faltantes:

Cuadro 4. Falencias Convenio Ciberdelincuencia

FALENCIAS ENCONTRADAS	DESCRIPCION
Falta Legislación sobre delitos informáticos	No juzga el delito sobre abuso de dispositivos
Falta Legislación sobre delitos informáticos	No juzga el delito sobre falsificación de información

Fuente: Los Autores

Al confrontar la Ley Colombiana con los delitos informáticos tipificados en el Convenio de Ciberdelincuencia se identificaron dos delitos que no son contemplados específicamente como lo tipifica el Convenio de Ciberdelincuencia, y en el análisis se observa que otros países como Perú y Venezuela si lo contemplan.

En Perú el Artículo 10 se denomina:Abuso de mecanismos y dispositivos informáticos, el cual castiga al que deliberadamente y fuera de la ley "fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley"[38]

Y en Venezuela también se legisla en contra de este delito, en el Artículo 10 de su normativa, el cual se denomina: "Posesión de equipos o prestación de servicios de sabotaje", y en el Artículo 20 "Posesión de equipo para falsificaciones"[39], que tiene similar concepto a la ley peruana.

[38]Normas Legales – El Peruano. (2014). *Ley No. 30171 – Ley que Modifica La Ley 30096, Ley de Delitos Informáticos.* Perú. Congreso de la República.
[39] Ley Especial Contra los Delitos Informáticos, Ven. § (2001).

Sí se examinan estas leyes a la luz del Convenio de Ciberdelincuencia, los conceptos concuerdan con la definición del delito Abuso de dispositivos.

Colombia toca el tema del "Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas"[40]en el Artículo 193 de la Ley 599 del 2000, pero no es suficiente para castigar todo lo que abarca el delito de Abuso de dispositivos.

Igualmente, el delito de Falsificación Informática, aunque la Ley Colombiana pueda catalogar la falsificación como un delito en el Art. 279 hasta el Art. 296 de la Ley 599 de 2000[40], del Código Penal, no obstante no determina la Falsificación informática como tal, habla de la falsificación de timbre oficial, de sellos, de documentos, etc. y cada Artículo precisa sus definiciones, pero no se puede ligar una falsificación informática en ninguno de los delitos sancionados en esta Ley.

En Argentina este delito de Falsificación es catalogado en el artículo 292[41] del Código Penal, el cual sin denotar específicamente el ser ejecutado mediante sistemas informáticos, su concepto es amplio como para cubrir los delitos informáticos.

En Costa Rica, el Artículo 217bis.-Estafa Informática define el mismo concepto que Falsificación Informática, de esta manera el delito es castigado. En Ecuador, el Artículo 60 que determina una modificación al Art. 353, cataloga específicamente la Falsificación electrónica dentro del concepto del delito de Falsificación informática. Y en Venezuela, el Artículo 12 llamado Falsificación de documentos, el cual concierne los sistemas y tecnologías de información dentro de su definición, también permite la sanción del delito de Falsificación Informática.

En conclusión, Colombia necesita que a su legislación se incorpore la sanción debida al delito de Falsificación informática para que se castigue a todo aquel que deliberadamente introduzca, altere o borre datos informáticos con el objeto de falsear la información.

Del Cuadro 2, de las sanciones por Delito se puede determinar que Colombia castiga con más severidad los delitos comparados que los 6 países restantes, los delitos que con mayor rigor castiga y multa son: fraude informático que va de 4 a 10 años prisión y multa de 200 a 1500 salario mínimos y la pornografía infantil que va de 10 a 20 años y multa de 150 a 1500 salarios mínimos legales, mientras que

[40]Ley 599 de 2000. *Código Penal Colombiano*, Col. § (2000).
[41] Legislación Argentina. *Código Penal Artículo 292.* Recuperado de: http://leyes-ar.com/codigo_penal/292.htm.

la legislación de Argentina el mismo delito Fraude Informático lo castiga de 1 mes a 6 años de prisión y la pornografía infantil de 6 meses a 4 años, y la legislación de Perú sanciona el delito de Fraude Informático de 3 a 8 años prisión y el delito de pornografía infantil lo castiga con 12 a 15 años de prisión, con esto se denota la mayor severidad en las sanciones por delito de la legislación Colombiana.

7.2CUADRO DE FORTALEZAS Y DEBILIDADES DE LA LEY 1273

Análisis de cada artículo en comparación con los Artículos relacionados en las diferentes legislaciones de los países seleccionados, que permitan establecer las fortalezas de la legislación colombiana y por ende sus debilidades, las cuales son transcritas en el Cuadro 5.

Cuadro 5.Fortalezas y Debilidades Ley 1273

LEY COLOMBIANA	FORTALEZAS	DEBILIDADES
ARTÍCULO 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO. En el cual se castiga al que sin estar autorizado o la fuerza acceda a un sistema informático.	Las sanciones impuestas son más drásticas a las sanciones impuestas en los demás países y la definición es más concreta y precisa.	La ley Colombiana no contempla el abuso a los dispositivos, no controla la creación de dispositivos utilizados en un delito.
ARTÍCULO 269B: OBSTACULIZACIÓNILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. Sanciona al que impide el funcionamiento normal de un sistema informático, o impide el acceso normal a una red de telecomunicación	Este artículo se creó para proteger un sistema informático del delito de extorsión informática.	El título no es explícito para definir su contenido, no especifica claramente el delito que pretende sancionar. No especifica la protección a la comunicación telegráfica, telefónicas o de la misma naturaleza.
ARTÍCULO 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. Se sanciona a aquel que intercepta datos informáticos sin tener una orden judicial para ello.	Este Artículo protege las emisiones electromagnéticas que provienen de un sistema en el territorio nacional	No contempla regulación de posesión de dispositivos que puedan utilizarse para cometer este delito. Se puede ampliar este Artículo haciendo referencia a la Interceptación de información con fines de extorción como lo especifica la Ley de Costa Rica en su Art. 214
ARTÍCULO 269D: DAÑO INFORMÁTICO. Se castiga al que destruye, daña, borra, deteriora, altera o suprime datos informáticos sin estar autorizado para ello	Contempla tanto los daños en los datos, en las partes lógicas y tangibles de un sistema informático.	No sanciona explícitamente a aquel que alterare, sustrajere, destruyere o inutilizare los objetos que puedan servir de prueba ante la autoridad competente, como lo especifica el Art. 255 de la ley Argentina.
ARTÍCULO 269E: USO DE SOFTWARE MALICIOSO. Sanciona al que trafica, produce, distribuye o vende programas maliciosos o software con efectos dañinos.	A través de este artículo se puede controlar las conductas delictivas que pueden tener algunos programadores cuando insertan virus que puedan destruir los programas para lucrarse del mal causado.	No define claramente una concientización del uso de este tipo de software.

Cuadro 5. (Continuación)

ARTÍCULO 269F: VIOLACIÓN DE DATOS PERSONALES. Se penaliza al que obteniendo datos personales o información privada de un tercero los emplea para su propio provecho.	**Colombia es uno de los primeros países en legislar a favor de la protección de los datos personales.**	**Sin comentario**
ARTÍCULO 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOSPERSONALES. Sanciona al que usa páginas electrónicas, enlaces o ventanas emergentes falsas para obtener datos confidenciales que usará para su beneficio	Protege al ciudadano del conocido "phishing" al caer infraganti en los spam que pueden ser usados para robar información.	Se puede ampliar este Artículo a la Suplantación de Identidad en las redes sociales o sitios de internet como lo menciona la Ley Costarricense en el Art. 230.
ARTÍCULO 269H: CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA. Describe los agravantes de las penas sí el delito se comete en redes o sistemas de organismos públicos, o en el sector financiero, sí es funcionario público, o contratistas que trabajan en el medio estatal, quien hace daño a un tercero revelando información confidencial, quien actúa con fines terroristas, se sanciona al administrador de sistemas de información que obra de mala fe con inhabilidad en sus funciones	Define los agravantes.	Se deja por fuera el espionaje.
ARTÍCULO 269I: HURTO POR MEDIOS INFORMÁTICOS y SEMEJANTES. Se castiga al que por medio de sistemas informáticos hurta, o suplanta a un usuario ante los sistemas de autenticación	Fortalece el Artículo 269G.	Sin comentario
ARTÍCULO 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS. Se sanciona al que manipulando un sistema transfiere activos perjudicando a un tercero, y lo hace para su propio lucro. Y también se sanciona al que fabrica, provee o facilita software que se utilice para realizar este tipo de delito.	Protege al Ciudadano Colombiano de la Estafa informática	El título debería haberse conservado como se presentó en el proyecto de Ley: Estafa Informática.
DELITO NO CONTEMPLADO		No se encuentran Artículos que puedan relacionar el Delito Informático con el Espionaje como lo menciona la Ley de Costa Rica en su Artículo 288 y en el Artículo 231 que habla propiamente del Espionaje Informático.
DELITO NO CONTEMPLADO		Falta especificar un artículo que castigue la Difusión de información falsa como lo regula Costa Rica en el Artículo 236.
NO CONTEMPLADO		Falta políticas de seguridad No se encuentra exigencias a entidades públicas o privadas para la implementaciones de sistemas de gestión de seguridad informática

Fuente: Los Autores

7.3IDENTIFICACIÓN DE FALENCIAS

Después de determinar las fortalezas y debilidades de cada artículo se pueden determinar algunas Falencias y Recomendaciones particulares a la Ley 1273 de 2009, las cuales se establecen en el Cuadro 6 descrito a continuación.

Cuadro 6. Falencias y Recomendaciones

LEY COLOMBIANA	FALENCIAS	RECOMENDACIONES
ARTÍCULO 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.	La ley Colombiana no contempla el abuso a los dispositivos, no controla la creación de dispositivos utilizados en un delito.	Se pueden realizar propuestas de ley basados en el delito de Abuso de dispositivos
ARTÍCULO 269B: OBSTACULIZACIÓNILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN.	El título no es explícito para definir su contenido, no especifica claramente el delito que pretende sancionar.	Ampliar los conceptos
ARTÍCULO 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS.	No contempla regulación de posesión de dispositivos que puedan utilizarse para cometer este delito. Se puede ampliar este Artículo haciendo referencia a la Interceptación de información con fines de extorción como lo especifica la Ley de Costa Rica en su Art. 214	Se pueden presentar proyectos de ley o creación de organizaciones del estado que se encarguen de controlar la adquisición de dispositivos que puedan emplearse en la interceptación de datos informáticos.
ARTÍCULO 269D: DAÑO INFORMÁTICO.	No sanciona explícitamente a aquel que alterare, sustrajere, destruyere o inutilizare los objetos que puedan servir de prueba ante la autoridad competente, como lo especifica el Art. 255 de la ley Argentina.	Se pueden realizar proyectos de ley basados la protección de cadenas de custodia de elementos informáticos probatorios en una investigación criminalística.
ARTÍCULO 269E: USO DE SOFTWARE MALICIOSO.	No define claramente una concientización del uso de este tipo de software.	El Estado puede promover el uso de software licenciado y la educación o concientización de las consecuencias del uso de software pirata.
ARTÍCULO 269F: VIOLACIÓN DE DATOS PERSONALES.	Sin Comentario	Sin Comentario
ARTÍCULO 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES	Se puede ampliar este Artículo a la Suplantación de Identidad en las redes sociales o sitios de internet como lo menciona la Ley Costarricense en el Art. 230.	El Estado puede proveer un cuerpo de policías cibernéticos especializados en la seguridad informática que controlen este flagelo.
ARTÍCULO 269H: CIRCUNSTANCIAS DE AGRAVACIÓN PUNITIVA.	Se deja por fuera el espionaje.	Se pueden presentar proyectos de Ley que Legislen sobre el espionaje informático
ARTÍCULO 269I: HURTO POR MEDIOS INFORMÁTICOS y SEMEJANTES.	Sin comentario	Sin comentario
ARTÍCULO 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.	El título debería haberse conservado como se presentó en el proyecto de Ley: Estafa Informática.	Proyecto de Ley que amplíe el significado de este Artículo para que sea de mayor aplicabilidad.

Cuadro 6. (Continuación)

DELITO NO CONTEMPLADO	**Delito de Espionaje Informático**	**Sancionar el Delito de Espionaje como lo menciona la Ley de Costa Rica en su Artículo 288 y en el Artículo 231 que habla propiamente del Espionaje Informático.**
DELITO NO CONTEMPLADO	Delito Difusión de Información Falsa	Sancionar la Difusión de información falsa como lo regula Costa Rica en el Artículo 236.
NO CONTEMPLADO	Obligatoriedad del uso de Políticas de Seguridad	Legislar el establecimiento de políticas de seguridad como exigencia en las entidades públicas o privadas para la implementación de sistemas de gestión de seguridad informática

Fuente: Los Autores

Del Cuadro 6 se pueden determinar los siguientes faltantes:

1. No existe legislación en contra del abuso de dispositivos

2. No se juzga el delito sobre falsificación de la Información

3. El título del Artículo 269B no expresa claramente el delito que legisla que es la extorsión informática.

4. El Artículo 269C no contempla la regulación de la posesión de dispositivos que se pueden utilizar para cometer este delito de interceptación de datos informáticos.
5. En el Artículo 269D No sanciona a aquel que altere, sustraiga, destruya o inutilice los objetos que puedan servir de prueba ante la autoridad competente.

6. El Artículo 269G se puede ampliar con la suplantación de Identidad en las redes sociales o sitios de internet.

7. El Artículo 269J debió conservar el nombre como se presentó en el proyecto de ley: Estafa Informática, para que el delito sea sancionado como tal.

8. Ausencia de Artículo que sancione el Espionaje Informático.

9. Falta una ley que castigue la difusión de información falsa a través de medios informáticos como lo regula Costa Rica en el Art. 236 de su Legislación.

10. No se encuentran exigencias que regulen Políticas de Seguridad en las instituciones del estado, que normalicé la implementen de Sistemas de Gestión de Seguridad Informática como lo regula Perú en su Legislación en las disposiciones complementarias.

7.4MARCO PARA LOS DELITOS FUTUROS

Sin demeritar el contenido de la Ley 1273 del 5 de enero de 2009 en Colombia y reconociendo el gran trabajo del reconocido Doctor Alexander Díaz García, Abogado Especialista Ciencias Penales y Criminológicas, Nuevas Tecnologías y Protección de Datos, entre otros estudios, y autor del Proyecto de Ley de Delitos Informáticos [42] , y resaltando el trabajo conjunto de los jurisprudentes que aprobaron esta Ley, respetuosamente se ha realizado la presente revisión teórica desde el punto de vista de los autores, fundados en el conocimiento adquirido en la Especialización de Seguridad Informática, básicamente en el curso de "Aspectos Éticos y Legales de Seguridad Informática", del análisis expuesto se pueden lograr otros puntos de vista que pueden ser explotados para mejorar la Legislación Colombiana.

Cabe destacar que la Ley Colombiana se ha constituido en un punto de referencia para otros países, porque a nivel internacional ha sido uno de los primeros en elevar a bien jurídico la Información y el dato[43], como lo explica su autor, es decir, la información y el dato se convierten en bienes protegidos por el derecho.

Aunque se aprobaron exitosamente 10 Artículos, se pueden mejorar aún más, como lo expuso el Doctor Díaz García en su Proyecto de Ley de Delitos Informáticos, en la cual expresaba con palabras más claras la tipificación de cada delito informático sobre el cual se legisla, al igual se dejaron por fuera tres

[42]Díaz A. (2010). *Aniversario en Colombia del nuevo Delito de Violación de Datos Personales.* Colombia. Alexander Díaz García.

[43] Díaz García, Alexander. (2008). *Proyecto de Ley de Delitos Informáticos.* Recuperado de http://nuevastecnologiasyprotecciondedatos.blogspot.com/2008/06/proyecto-de-ley-delitos-informticos_17.html .

artículos que el autor proponía que son de gran importancia sobre los cuales se podría argumentar legalmente:

- Falsedad Informática
- Espionaje Informático
- Spam (correo no deseado)

Y no solamente estos delitos, sino todos aquellos que se van tipificando por el constante crecimiento de nuevas formas de delinquir en contra de la seguridad informática, como por ejemplo:

- El Bullying Informático
- El Mobbing Informático

Pero la idea propuesta a través de este estudio es la concientización de la importancia de incluir en la legislación colombiana políticas de Seguridad Informática como lo hizo el país con Legislación más reciente, Perú, la Ley Peruana en cuanto a Delitos Informáticos es muy completa, gran parte de su estudio se basa en el Convenio de Ciberdelincuencia del 2001, y se fortalece mucho más cuando establece una disposición que particularmente promueve el uso de Medidas de Seguridad para la protección de los datos y su integridad, y las buenas prácticas.

7.5 PLANTEAMIENTO DE MEJORAS A LA LEY 1273 EN LA LEGISLACIÓN NACIONAL DE COLOMBIA

En el Cuadro 7 se plasma la Ley 1273 de 2009 en cada uno de sus Artículos, en el cual se plantean mejoras en los títulos y en el contenido de cada uno, las modificaciones aparecen en color rojo y subrayado, todo el texto restante se transcribe tal y como se encuentra en cada artículo de la Ley denominada “de la protección de la información y de los datos”[44].

Estas mejoras se plantean con el fin de manifestar un punto de vista de los autores basados en el conocimiento adquirido en la Especialización de Seguridad Informática y para exponer teóricamente la necesidad de modificar la Ley sobre Delitos Informáticos en Colombia, para que los artículos sean más específicos,

[44] Ley 1273 de 2009. *De la Protección de la información y de los datos*, Col. § 269 (2009).

entendibles, con proyección internacional y más fáciles de interpretar para que exista un tipificación del delito más efectiva.

Cuadro 7. Planteamiento de Mejoras a la Ley 1273

LEY COLOMBIANA	PLANTEAMIENTO PROPUESTO	CONTENIDO
ARTÍCULO 269A: ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.	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.	ARTÍCULO 269B: EXTORSION INFORMÁTICA	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 telecomunicacionescon el fin de lucro personal, 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.	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.	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 altere, sustraiga, destruya o inutilice los objetos que puedan servir de prueba ante la autoridad competente, 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.	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.

Cuadro 7. (Continuación)

ARTÍCULO 269F: VIOLACIÓN DE DATOS PERSONALES.	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	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. La misma sanción será aplicada al que suplante identidad en redes sociales o sitios de internet. 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.	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.

Cuadro 7. (Continuación)

ARTÍCULO 269I: HURTO POR MEDIOS INFORMÁTICOS y SEMEJANTES.	**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.	ARTÍCULO 269J: ESTAFA INFORMATICA	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 ADICIONAL	ARTICULO 269K: ABUSO DE DISPOSITIVOS	"El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito" [45] 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[46]
ARTÍCULO ADICIONAL	ARTÍCULO 269L: FALSIFICACION INFORMATICA	El que sin autorización para ello y valiéndose de cualquier medio electrónico, borre, altere, suprima, modifique o inutilice los datos registrados en una computadora, incurrirá en prisión de cuatro (4) a ocho (8) años y en multa de 50 a 500 salarios mínimos legales mensuales vigentes.[47]

[45] Normas Legales – El Peruano. (2014). *Ley No. 30171 – Ley que Modifica La Ley 30096, Ley de Delitos Informáticos – Artículo 10.* Perú. Congreso de la República.
[46] MinTIC. (2009). *Ley 1273 de 2009 – Sanción del Artículo 269F.* Colombia. Ministerio de Tecnologías de la Información y las Comunicaciones.
[47] Díaz García, Alexander. (2008). *Proyecto de Ley de Delitos Informáticos – Artículo 269H.* Recuperado de http://nuevastecnologiasyprotecciondedatos.blogspot.com/2008/06/proyecto-de-ley-delitos-informticos_17.html

Cuadro 7. (Continuación)

ARTÍCULO ADICIONAL	ARTÍCULO 269M: ESPIONAJE INFORMÁTICO	"El que se apodere, interfiera, transmita, copie, modifique, destruya, utilice, impida o recicle datos informáticos de valor para el tráfico económico de la industria, el comercio, o datos de carácter político y/o militar relacionados con la seguridad del Estado, incurrirá en prisión de seis (6) a diez (10) años y multa de 500 a 2.500 salarios legales mínimos mensuales vigentes"[48].
ARTÍCULO ADICIONAL	ARTÍCULO 269N: DIFUSIÓN DE INFORMACIÓN FALSA	El que "a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios."[49]Incurrirá en prisión de cuatro (4) a ocho (8) años y en multa de 50 a 500 salarios mínimos legales mensuales vigentes.[50]
PARAGRAFO ADICIONAL	PARAGRAFO 1:	Legíslese a favor de la Seguridad Informática en toda institución del Gobierno Nacional y sea de obligatorio cumplimiento para preservación de la Información y los datos.

Fuente: Los Autores

En resumidas cuentas, del cuadro 7 se pueden plantear las siguientes mejoras:

- Modifíquese el título del Artículo 269B como **Extorción Informática.** Y adiciónese a la definición del delito el texto "con el fin de lucro personal".

- En el Artículo 269D, adiciónese a la definición del delito el texto "o altere, sustraiga, destruya o inutilice los objetos que puedan servir de prueba ante la autoridad competente".

- En el Artículo 269G, adiciónese a la definición del delito, el texto "La misma sanción será aplicada al que suplante identidad en redes sociales o sitios de internet".

[48] Díaz García, Alexander. (2008). *Proyecto de Ley de Delitos Informáticos – Artículo 269A.* Recuperado de http://nuevastecnologiasyprotecciondedatos.blogspot.com/2008/06/proyecto-de-ley-delitos-informticos_17.html

[49]Sistema Costarricense de Información Jurídica. (2012). *Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal N° 9048 – Artículo 236.* Costa Rica. Asamblea Legislativa de la República de Costa Rica.

[50] Díaz García, Alexander. (2008). *Proyecto de Ley de Delitos Informáticos – Sanción Artículo 269H.* Recuperado de http://nuevastecnologiasyprotecciondedatos.blogspot.com/2008/06/proyecto-de-ley-delitos-informticos_17.html

- Modifíquese el título del Artículo 269J por **Estafa Informática.**

- Incorpórese el Artículo 269K: **Abuso de Dispositivos.** "El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito" [51] 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[52].

- Incorpórese el Artículo 269L: **Falsificación Informática**. El que sin autorización para ello y valiéndose de cualquier medio electrónico, borre, altere, suprima, modifique o inutilice los datos registrados en una computadora, incurrirá en prisión de cuatro (4) a ocho (8) años y en multa de 50 a 500 salarios mínimos legales mensuales vigentes.[53]

- Incorpórese el Artículo 269M: **Espionaje Informático.**"El que se apodere, interfiera, transmita, copie, modifique, destruya, utilice, impida o recicle datos informáticos de valor para el tráfico económico de la industria, el comercio, o datos de carácter político y/o militar relacionados con la seguridad del Estado, incurrirá en prisión de seis (6) a diez (10) años y multa de 500 a 2.500 salarios legales mínimos mensuales vigentes"[54].

- Incorpórese el Artículo 269N: **Difusión de Información falsa.** El que "a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones, propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema

[51] Normas Legales – El Peruano. (2014). *Ley No. 30171 – Ley que Modifica La Ley 30096, Ley de Delitos Informáticos – Artículo 10.* Perú. Congreso de la República.
[52]MinTIC. (2009). *Ley 1273 de 2009 – Sanción del Artículo 269F.* Colombia. Ministerio de Tecnologías de la Información y las Comunicaciones.
[53] Díaz García, Alexander. (2008). *Proyecto de Ley de Delitos Informáticos – Artículo 269H.* Recuperado de http://nuevastecnologiasyprotecciondedatos.blogspot.com/2008/06/proyecto-de-ley-delitos-informticos_17.html
[54] Díaz García, Alexander. (2008). *Proyecto de Ley de Delitos Informáticos – Artículo 269A.* Recuperado de http://nuevastecnologiasyprotecciondedatos.blogspot.com/2008/06/proyecto-de-ley-delitos-informticos_17.html

financiero o de sus usuarios."[55]Incurrirá en prisión de cuatro (4) a ocho (8) años y en multa de 50 a 500 salarios mínimos legales mensuales vigentes.[56]

- Incorpórese el Parágrafo 1: Legíslese a favor de la Seguridad Informática en toda institución del Gobierno Nacional y sea de obligatorio cumplimiento para preservación de la Información y los datos.

[55]Sistema Costarricense de Información Jurídica. (2012). *Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal N° 9048 – Artículo 236.* Costa Rica. Asamblea Legislativa de la República de Costa Rica.

[56] Díaz García, Alexander. (2008). *Proyecto de Ley de Delitos Informáticos – Sanción Artículo 269H.* Recuperado de http://nuevastecnologiasyprotecciondedatos.blogspot.com/2008/06/proyecto-de-ley-delitos-informticos_17.html

CONCLUSIONES

- ✓ Se concluye que a la Legislación Colombiana le hace falta el tratamiento de algunos delitos que han sido establecidos en el Convenio de Ciberdelincuencia de las Naciones Unidas, como son: Abuso de dispositivos y Falsificación de Información.

- ✓ Se concluye que Colombia al no hacer parte activa del Convenio de Ciberdelincuencia provoca que tenga falencias en su normativa jurídica ya que no asocia las definiciones de delitos informáticos con los términos que ya se han definido a nivel internacional.

- ✓ También se concluye que no existe un organismo de control especializado que se haya establecido desde la Legislación Colombiana encargado de asegurar el tratamiento de los Delitos Informáticos.

- ✓ De acuerdo a la búsqueda de información realizada,se concluye que en Colombia se han cometido muchos delitos informáticos que no han sido castigados de la forma adecuada porque no se encuentran bien tipificados en la norma.

- ✓ Se concluye que las mejoras mostradas como resultado de este estudio pueden servir como base para formular proyectos de Ley de futuras legislaciones en cuanto a la tipificación de delitos informáticos.

- ✓ Mediante el estudio realizado se concluye que las falencias principales de la Ley 1273 de 2009 se encuentran:
- En su contenido, porque existen delitos que deberían contemplarse.
- En las definiciones de los delitos, porque existiendo definiciones en tratados internacionales no se los utiliza plenamente
- En la tipificación específica de los delitos, porque los títulos como se los conoce no son comprensibles a todo lector.

RECOMENDACIONES

- ✓ Impulsar la creación de proyectos de Ley en los que se incluyan los delitos informáticos de Abuso de dispositivos, Falsificación Informática, Espionaje Informático, Difusión de Información falsa, basados en los nuevos puntos de vista plasmados en la presente Monografía.

- ✓ Concientizara los Autores Legislativos de que Colombia necesita ratificar su alianza al Convenio de Ciberdelincuencia de 2001, para que su legislación adopte los conceptos universales que se manejan sobre delitos informáticos, esto permitirá que a la hora de tipificar un delito se señale en un término que otros países también puedan reconocer.

- ✓ La legislación Colombiana necesita promover jurídicamente la adopción de políticas de Seguridad Informática y Sistemas de Gestión de Seguridad Informática a los entes de administración pública en primera instancia, para salvaguardar la información de la ciudadanía en general de la cual son custodios, y en segunda instancia extender la normativa hacia los entes privados para protección de su valiosa información ante un eventual ataque de ciberdelincuencia.

BIBLIOGRAFIA

Acurio, S. *Delitos Informáticos*: *Generalidades.* Quito – Ecuador. Pontificia Universidad Católica del Ecuador (PUCE).

Alvarado E., Borges, B. (2004). *Guía práctica para el desarrollo de monografías, ensayos, bibliografías y extractos*. Puerto Rico. Publicaciones Puertorriqueñas.

Archivo General de la Nación. (2014). Normativa. Recuperado de: http://www.archivogeneral.gov.co/normativa.

Ayuntamiento de Calahorra (2013). *Glosario de Términos relacionados con Delitos Informáticos.* Recuperado de http://www.educacion.gob.es/exterior/centros/ginerdelosrios/es/internet-seguro/DiccionarioDelitosTecnologicos.pdf

Becerra R. (2011). *Delitos Informáticos en México en espera de una Ley*. Recuperado de: http://www.sdpnoticias.com/columnas/2011/08/15/delitos-informaticos-en-mexico-en-espera-de-una-ley.

Borgello, C. F. (2011). *Legislaciones y Principios de Privacidad del primer mundo*. Recuperado de http://www.segu-info.com.ar/articulos/105-principios-privacidad.htm.

Calderón R, Guzmán G, Salinas J. (2011). *Diseño y Plan de Implementación de un Laboratorio de Ciencias Forenses Digitales Tesina de Seminario.* Guayaquil – Ecuador. Escuela Superior Politécnica del Litoral.

Carlos 1234 (2012). *Países más Poderosos de América Latina.* Recuperado de http://listas.20minutos.es/lista/paises-mas-poderosos-de-america-latina-337996/

Código Penal Online. *Código Penal de la Nación Argentina*. Recuperado de http://www.codigopenalonline.com.ar/codigo_penal_argentino_delitos_contra_la_propiedad.html.

Córdoba J. (2012). *Nueva ley de Delitos Informáticos en Costa Rica. Costa Rica*. Ticoblogger. Recuperado de http://ticoblogger.com/2012/07/11/delitos-informaticos-costa-rica/.

Definición abc. (2007). *Definición de Spam*. Recuperado de: http://www.definicionabc.com/tecnologia/spam.php#ixzz3FJxSqofj.

Definición.de. (2008). *Definición de Peculado*. Recuperado de http://definicion.de/peculado/.

Depósito de documentos de la FAO. (2013). *América Latina y El Caribe.* Recuperado de: http://www.fao.org/docrep/v8300s/v8300s0o.htm.

Díaz García, Alexander. (2008). *Proyecto de Ley de Delitos Informáticos.* Recuperado de http://nuevastecnologiasyprotecciondedatos.blogspot.com/2008/06/proyecto-de-ley-delitos-informticos_17.html .

Díaz A. (2010). *Aniversario en Colombia del nuevo Delito de Violación de Datos Personales.* Colombia. Alexander Díaz García.

División ComputerForensic, (2012). *Definición de Delito Informático.* Recuperado de http://delitosinformaticos.info/delitos_informaticos/definicion.html.

Ecuador. (06 de Enero de 2014). *Se tipifican los delitos informáticos en el nuevo Código Penal del Ecuador*. Movistar. Recuperado de http://www.movistar.com.ec/comunidad/showthread.php?514-Se-tipifican-los-delitos-inform%E1ticos-en-el-nuevo-C%F3digo-Penal-del-Ecuador.

Ecixgroup (2012). *Brasil aprueba primera ley contra delitos informáticos.* Recuperado de: https://ecixgroup.com/brasil-aprueba-primera-ley-contra-delitos-informaticos/

El Derecho en su interpretación Judicial. (2008). *Prohibición de la aplicación de la Analogía*. Jurisprudencia Penal.

García Y, Gamboa M. (2011). Lineamientos para Trabajos de Grado. Bogotá D.C. Universidad Nacional Abierta y a Distancia – UNAD.

Guarnizo M, (2012). *Delitos informáticos en el Código Penal Peruano*. Recuperado de: http://ao2011actividadesdeeducarte.blogspot.com/2012/07/delitos-informaticos-en-el-codigo-penal.html.

ICONTEC - Instituto Colombiano De Normas Técnicas y Certificación (2008). *Trabajos escritos: presentación y referencias bibliográficas*. Sexta actualización. Bogotá.

InfoLeg - Información Legislativa. (2000). *Código Penal Ley 25.326 – Artículo 32.* Argentina. Ministerio de Economía y Finanzas Públicas.

InfoLeg - Información Legislativa. (2008). *Código Penal Ley 26.388.* Argentina. Ministerio de Economía y Finanzas Públicas.

Legislación Argentina. *Código Penal Artículo 292.* Recuperado de: http://leyes-ar.com/codigo_penal/292.htm.

Ley 599 de 2000. *Código Penal Colombiano,* Col. § (2000).

Ley 1273 de 2009. *De la Protección de la información y de los datos*, Col. § 269 (2009).

Ley 1336 de 2009. *Protección de Datos Personales*, Col. § 218 (2009).

Ley Especial Contra los Delitos Informáticos, Ven. § (2001).

Ley No. 2002-67, Registro Oficial 557-S, Ecu § (2002).

Manson, M. (2007). *Legislación sobre delitos informáticos*. Recuperado de http://www.monografias.com/trabajos/legisdelinf/legisdelinf.shtml.

Ministerio de Justicia (1993). *Ley Relativa a Delitos Informáticos.* Chile. Biblioteca del Congreso Nacional.

Ministerio de Justicia (2003). *Ley 19927Modifica el código penal, el código de procedimiento penal y el código procesal penal en materia de delitos de pornografía infantil.* Chile. Biblioteca del Congreso Nacional

Min TIC. (2009). *Ley 1273 de 2009.* Colombia. Ministerio de Tecnologías de la Información y las Comunicaciones.

Monografías. *Definiciones de Delito*. Recuperado de http://www.todoiure.com.ar/monografias/mono/penal/Definiciones_de_delito.htm.

Normas Legales – El Peruano. (2013). *Ley No. 30096 – Ley de Delitos Informáticos.* Perú. Congreso de la República.

Normas Legales – El Peruano. (2014). *Ley No. 30171 – Ley que Modifica La Ley 30096, Ley de Delitos Informáticos.* Perú. Congreso de la República.

Orlando. (2010). *Legislación Boliviana en Materia de Delitos Informáticos*. Recuperado de: http://legisbol.blogspot.com/2010/06/5-legislacion-boliviana-en-materia-de.html.

Panda Security (2014). *Phishing*. Recuperado de: http://www.pandasecurity.com/colombia/homeusers/security-info/cybercrime/phishing/.

Pérez F. (2012). *Ley 1273 de 2009 y Delitos Informáticos tipificados en el Código Penal.* Colombia. Recuperado de http://es.slideshare.net/german1537/aspectos-informaticos-relevantes-ley-1273-de-2009.

Proz.com. (2007). *Terminology*. Recuperado de: http://www.proz.com/kudoz/spanish_to_english/law_general/2297422-agravaci%C3%B3n_punitiva.html.

Reyes P. (1999). Análisis y diseño de sistemas, caso SIABUC. Colombia. Universidad de Colima.

Sabogal Rozo, E. (2013). *Módulo Proyecto Seguridad Informática*. La Plata Huila: Universidad Nacional Abierta y a Distancia.

Santos & Rojas Abogados. (2004). Tipos de Delitos Informáticos. Recuperado de: http://www.abogadosantosrojas.com/delitos/tiposdelitos.php.

Seguridad de la Información. *Legislación y Delitos Informáticos* - La Información y el Delito. Recuperado de http://www.segu-info.com.ar/legislacion/

Seguridad de la Información. *Legislación y Delitos Informáticos.* Recuperado de http://www.segu-info.com.ar/delitos/delitos.htm

Seguridadpc.net. Concepto de Virus Informáticos. Recuperado de http://www.seguridadpc.net/introd_antiv.htm.

Serie de Tratados Europeos-n° 185. *Convenio sobre la Ciberdelincuencia.* Budapest, Concilio de Europa.

Significados. (2013). *Significado de Bullying*. Recuperado de http://www.significados.com/bullying/.

Solarte F, Gonzalez Y. (2013). *Módulo Aspectos Éticos y legales de Seguridad Informática*. CEAD Pasto, CEAD Arbealez. Universidad Nacional Abierta y a Distancia – UNAD.

Temperini, Marcelo Gabriel Ignacio. (2013). *Delitos Informáticos en Latinoamérica: Un estudio comparado. 1ra. Parte*. Argentina. Universidad Nacional del Litoral.

Universia. (1990). *¿Qué es el Mobbing?.* Recuperado de http://contenidos.universia.es/especiales../mobbing/concepto/index.htm

Umaña R. (2010). *Delitos Informáticos*. Costa Rica. Universidad de Costa Rica.

Zavala Trías S. (2012). *Guía a la redacción en el estilo APA, 6ta edición.* San Juan de Puerto Rico. Universidad Metropolitana UMET.

ANEXOS

Por la extensión de las legislaciones se toman los Artículos referentes a los Delitos Informáticos, se proporciona la URL para descargar los documentos completos.

ANEXO A. Legislación Delitos Informáticos en Colombia

Ley 1273 del 05 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

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.

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.

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.

Artículo 58. Circunstancias 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[57].

Descargar Documento completo en:

http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

[57]MinTIC. (2009). *Ley 1273 de 2009.* Colombia. Ministerio de Tecnologías de la Información y las Comunicaciones

ANEXO B.LEY 1336 DE 2009 de 21 de julio de 2009

Ley 1336 del 2009 por medio del cual se adiciona y robustece la ley 679 de 2001 de lucha contra la explotación la pornografía y turismo sexual con niños, niñas y adolescentes establece 28 artículos donde regula el servicio turístico, aerolíneas y pornografía infantil en su artículo 24 que es el que se contempla en la monografía.

ARTÍCULO 24. El artículo 218 de la ley 599 quedará así:

Artículo 218. Pornografía con personas menores de 18 años. El que fotografíe, filme, grabe, produzca, divulgue, ofrezca, venda, compre, posea, porte, almacene, trasmita o exhiba, por cualquier medio, para uso personal o intercambio, representaciones reales de actividad sexual que involucre persona menor de 18 años de edad, incurrirá en prisión de 10 a 20 años y multa de 150 a 1.500 salarios mínimos legales mensuales vigentes[58].

Descargar Documento completo en:
http://www.mincit.gov.co/descargar.php?idFile=2350

ANEXO C. Legislación Delitos Informáticos en Argentina

La Ley 25326, de Protección de Datos Personales del 30 de Octubre del 2000.

ARTICULO 32. — (Sanciones penales).

1. Incorpórase como artículo 117 bis del Código Penal, el siguiente:

"1°. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.

2°. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.

[58]Ley 1336 de 2009. *Protección de Datos Personales*, Col. § 218 (2009).

3°. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.

4°. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena".

2. Incorpórase como artículo 157 bis del Código Penal el siguiente:

"Será reprimido con la pena de prisión de un mes a dos 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°. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años". [59]

Descargar Documento completo en:

http://www.oas.org/juridico/PDFs/arg_ley25326.pdf

ANEXO D.Ley 26388 de Delitos Informáticos del 2008

CODIGO PENAL ARGENTINA

Ley 26.388

Modificación.

Sancionada: Junio 4 de 2008

Promulgada de Hecho: Junio 24 de 2008

[59]InfoLeg - Información Legislativa. (2000). Código Penal Ley 25.326 – Artículo 32. Argentina. Ministerio de Economía y Finanzas Públicas.

El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:

ARTICULO 1º — Incorpórense 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 DIAS DEL MES DE JUNIO DEL AÑO DOS MIL OCHO.

— REGISTRADO BAJO EL Nº 26.388 —

EDUARDO A. FELLNER. — JULIO C. C. COBOS. — Enrique Hidalgo. — Juan H. Estrada.[60]

Descargar Documento completo en:

http://new.pensamientopenal.com.ar/01072008/codigos04.pdf

ANEXO E. Legislación Delitos Informáticos en Costa Rica

Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código PenalN° 9048 de 2012.

ARTÍCULO 1.-

Refórmense los artículos 167, 196, 196 bis, 214, 217 bis, 229 bis y 288 de la Ley N.º 4573, Código Penal, de 4 de mayo de 1970, y sus reformas. Los textos dirán:

“Artículo 167.- Corrupción

Será sancionado con pena de prisión de tres a ocho años quien mantenga o promueva la corrupción de una persona menor de edad o incapaz, con fines eróticos, pornográficos u obscenos, en exhibiciones o espectáculos públicos o privados, aunque la persona menor de edad o incapaz lo consienta.

La pena será de cuatro a diez años de prisión, si el actor, utilizando las redes sociales o cualquier otro medio informático o telemático, u otro medio de comunicación, busca encuentros de carácter sexual para sí, para otro o para grupos, con una persona menor de edad o incapaz; utiliza a estas personas para promover la corrupción o las obliga a realizar actos sexuales perversos, prematuros o excesivos, aunque la víctima consienta participar en ellos o verlos ejecutar.”

“Artículo 196.- Violación de correspondencia o comunicaciones

[60]InfoLeg - Información Legislativa. (2008). *Código Penal Ley 26.388.* Argentina. Ministerio de Economía y Finanzas Públicas

Será reprimido con pena de prisión de tres a seis años quien, con peligro o daño para la intimidad o privacidad de un tercero, y sin su autorización, se apodere, accese, modifique, altere, suprima, intervenga, intercepte, utilice, abra, difunda o desvíe de su destino documentos o comunicaciones dirigidos a otra persona.

La pena será de cuatro a ocho años de prisión si las conductas descritas son realizadas por:

a) Las personas encargadas de la recolección, entrega o salvaguarda de los documentos o comunicaciones.

b) Las personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

Artículo 196 bis.- Violación de datos personales

Será sancionado con pena de prisión de tres a seis años quien en beneficio propio o de un tercero, con peligro o daño para la intimidad o privacidad y sin la autorización del titular de los datos, se apodere, modifique, interfiera, acceda, copie, transmita, publique, difunda, recopile, inutilice, intercepte, retenga, venda, compre, desvíe para un fin distinto para el que fueron recolectados o dé un tratamiento no autorizado a las imágenes o datos de una persona física o jurídica almacenados en sistemas o redes informáticas o telemáticas, o en contenedores electrónicos, ópticos o magnéticos.

La pena será de cuatro a ocho años de prisión cuando las conductas descritas en esta norma:

a) Sean realizadas por personas encargadas de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tengan acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

b) Cuando los datos sean de carácter público o estén contenidos en bases de datos públicas.

c) Si la información vulnerada corresponde a un menor de edad o incapaz.

d) Cuando las conductas afecten datos que revelen la ideología, la religión, las creencias, la salud, el origen racial, la preferencia o la vida sexual de una persona.”

“Artículo 214.- Extorsión

Será reprimido con pena de prisión de cuatro a ocho años al que para procurar un lucro obligue a otro, con intimidación o con amenazas graves, a tomar una disposición patrimonial perjudicial para sí mismo o para un tercero.

La pena será de cinco a diez años de prisión cuando la conducta se realice valiéndose de cualquier manipulación informática, telemática, electrónica o tecnológica.”

“Artículo 217 bis.- Estafa informática

Se impondrá prisión de tres a seis años a quien, en perjuicio de una persona física o jurídica, manipule o influya en el ingreso, en el procesamiento o en el resultado de los datos de un sistema automatizado de información, ya sea mediante el uso de datos falsos o incompletos, el uso indebido de datos, programación, valiéndose de alguna operación informática o artificio tecnológico, o bien, por cualquier otra acción que incida en el procesamiento de los datos del sistema o que dé como resultado información falsa, incompleta o fraudulenta, con la cual procure u obtenga un beneficio patrimonial o indebido para sí o para otro.

La pena será de cinco a diez años de prisión, si las conductas son cometidas contra sistemas de información públicos, sistemas de información bancarios y de entidades financieras, o cuando el autor es un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.”

“Artículo 229 bis.- Daño informático

Se impondrá pena de prisión de uno a tres años al que sin autorización del titular o excediendo la que se le hubiera concedido y en perjuicio de un tercero, suprima, modifique o destruya la información contenida en un sistema o red informática o telemática, o en contenedores electrónicos, ópticos o magnéticos.

La pena será de tres a seis años de prisión, si la información suprimida, modificada, destruida es insustituible o irrecuperable.”

“Artículo 288.- Espionaje

Será reprimido con prisión de cuatro a ocho años al que procure u obtenga indebidamente informaciones secretas políticas o de los cuerpos de policía nacionales o de seguridad concernientes a los medios de defensa o a las

relaciones exteriores de la nación, o afecte la lucha contra el narcotráfico o el crimen organizado.

La pena será de cinco a diez años de prisión cuando la conducta se realice mediante manipulación informática, programas informáticos maliciosos o por el uso de tecnologías de la información y la comunicación.”

“Artículo 229.- Daño agravado

Se impondrá prisión de seis meses a cuatro años:

6) Cuando el daño recayera sobre redes, sistemas o equipos informáticos, telemáticos o electrónicos, o sus componentes físicos, lógicos o periféricos."

“Artículo 229 ter.- Sabotaje informático

Se impondrá pena de prisión de tres a seis años al que, en provecho propio o de un tercero, destruya, altere, entorpezca o inutilice la información contenida en una base de datos, o bien, impida, altere, obstaculice o modifique sin autorización el funcionamiento de un sistema de tratamiento de información, sus partes o componentes físicos o lógicos, o un sistema informático.

La pena será de cuatro a ocho años de prisión cuando:

a) Como consecuencia de la conducta del autor sobrevenga peligro colectivo o daño social.

b) La conducta se realice por parte de un empleado encargado de administrar o dar soporte al sistema o red informática o telemática, o bien, que en razón de sus funciones tenga acceso a dicho sistema o red, o a los contenedores electrónicos, ópticos o magnéticos.

c) El sistema informático sea de carácter público o la información esté contenida en bases de datos públicas.

d) Sin estar facultado, emplee medios tecnológicos que impidan a personas autorizadas el acceso lícito de los sistemas o redes de telecomunicaciones.”

Artículo 230.- Suplantación de identidad

Será sancionado con pena de prisión de tres a seis años quien suplante la identidad de una persona en cualquier red social, sitio de Internet, medio electrónico o tecnológico de información. La misma pena se le impondrá a quien, utilizando una identidad falsa o inexistente, cause perjuicio a un tercero.

La pena será de cuatro a ocho años de prisión si con las conductas anteriores se causa un perjuicio a una persona menor de edad o incapaz.

Artículo 231.- Espionaje informático

Se impondrá prisión de tres a seis años al que, sin autorización del titular o responsable, valiéndose de cualquier manipulación informática o tecnológica, se apodere, transmita, copie, modifique, destruya, utilice, bloquee o recicle información de valor para el tráfico económico de la industria y el comercio.

Artículo 232.- Instalación o propagación de programas informáticos maliciosos

Será sancionado con prisión de uno a seis años quien sin autorización, y por cualquier medio, instale programas informáticos maliciosos en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos.

La misma pena se impondrá en los siguientes casos:

a) A quien induzca a error a una persona para que instale un programa informático malicioso en un sistema o red informática o telemática, o en los contenedores electrónicos, ópticos o magnéticos, sin la debida autorización.

b) A quien, sin autorización, instale programas o aplicaciones informáticas dañinas en sitios de Internet legítimos, con el fin de convertirlos en medios idóneos para propagar programas informáticos maliciosos, conocidos como sitios de Internet atacantes.

c) A quien, para propagar programas informáticos maliciosos, invite a otras personas a descargar archivos o a visitar sitios de Internet que permitan la instalación de programas informáticos maliciosos.

d) A quien distribuya programas informáticos diseñados para la creación de programas informáticos maliciosos.

e) A quien ofrezca, contrate o brinde servicios de denegación de servicios, envío de comunicaciones masivas no solicitadas, o propagación de programas informáticos maliciosos.

La pena será de tres a nueve años de prisión cuando el programa informático malicioso:

i) Afecte a una entidad bancaria, financiera, cooperativa de ahorro y crédito, asociación solidarista o ente estatal.

ii) Afecte el funcionamiento de servicios públicos.

iii) Obtenga el control a distancia de un sistema o de una red informática para formar parte de una red de ordenadores zombi.

iv) Esté diseñado para realizar acciones dirigidas a procurar un beneficio patrimonial para sí o para un tercero.

v) Afecte sistemas informáticos de la salud y la afectación de estos pueda poner en peligro la salud o vida de las personas.

vi) Tenga la capacidad de reproducirse sin la necesidad de intervención adicional por parte del usuario legítimo del sistema informático.

Artículo 233.- Suplantación de páginas electrónicas

Se impondrá pena de prisión de uno a tres años a quien, en perjuicio de un tercero, suplante sitios legítimos de la red de Internet.

La pena será de tres a seis años de prisión cuando, como consecuencia de la suplantación del sitio legítimo de Internet y mediante engaño o haciendo incurrir en error, capture información confidencial de una persona física o jurídica para beneficio propio o de un tercero.

Artículo 234.- Facilitación del delito informático

Se impondrá pena de prisión de uno a cuatro años a quien facilite los medios para la consecución de un delito efectuado mediante un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos.

Artículo 235.- Narcotráfico y crimen organizado

La pena se duplicará cuando cualquiera de los delitos cometidos por medio de un sistema o red informática o telemática, o los contenedores electrónicos, ópticos o magnéticos afecte la lucha contra el narcotráfico o el crimen organizado.

Artículo 236.- Difusión de información falsa

Será sancionado con pena de tres a seis años de prisión quien, a través de medios electrónicos, informáticos, o mediante un sistema de telecomunicaciones,

propague o difunda noticias o hechos falsos capaces de distorsionar o causar perjuicio a la seguridad y estabilidad del sistema financiero o de sus usuarios."[61]

Descargar Documento completo en:

http://www.poder-judicial.go.cr/salatercera/index.php/leyes/category/4-legislacion-especial-relacionada-con-la-materia-penal?download=456:ley-9048-11-2012

ANEXO F. Legislación Delitos Informáticos en Chile

Ley 19223contra los "Delitos Informáticos" del 28 de Mayo de 1993.

Artículo 1º.- 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 2º.- 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 3º.- 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 4º.- 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."[62].

[61]Sistema Costarricense de Información Jurídica. (2012). *Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código PenalN° 9048.* Costa Rica. Asamblea Legislativa de la República de Costa Rica

[62]Ministerio de Justicia (1993). *Ley Relativa a Delitos Informáticos.* Chile. Biblioteca del Congreso Nacional.

Descargar Documento completo en:

http://www.leychile.cl/Navegar?idNorma=30590&idVersion=1993-06-07

ANEXO G.LEY NUM. 19.927, promulgada el 05 de enero de 2004.

MODIFICA EL CODIGO PENAL, EL CODIGO DE PROCEDIMIENTO PENAL Y EL CODIGO PROCESAL PENALEN MATERIA DE DELITOS DE PORNOGRAFIA INFANTIL

"Artículo 365 bis.- Si la acción sexual consistiere en la introducción de objetos de cualquier índole, por vía vaginal, anal o bucal, o se utilizaren animales en ello, será castigada:

1.- con presidio mayor en su grado mínimo a medio, si concurre cualquiera delas circunstancias enumeradas en el artículo 361;

2.- Con presidio mayor en cualquiera de sus grados, si la víctima fuere menor de catorce años, y 3.- con presidio menor en su grado máximo a presidio mayor en sugrado mínimo, si concurre alguna de las circunstancias enumeradas en el artículo363 y la víctima es menor de edad, pero mayor de catorce años.".

"Artículo 366.- El que abusivamente realizare una acción sexual distinta del acceso carnal con una persona mayor de catorce años, será castigado con presidio menor en su grado máximo, cuando el abuso consistiere en la concurrencia de alguna de las circunstancias enumeradas en el artículo 361.

Igual pena se aplicará cuando el abuso consistiere en la concurrencia de alguna de las circunstancias enumeradas en el artículo 363, siempre que la víctima fuere mayor de catorce y menor de dieciocho años.".

"Artículo 366 bis.- El que realizare una acción sexual distinta del acceso carnal con una persona menor de catorce años, será castigado con la pena de presidio menor en su grado máximo a presidio mayor en su grado mínimo.".

"Artículo 366 quáter.- El que, sin realizar una acción sexual en los términos anteriores, para procurar su excitación sexual o la excitación sexual de otro, realizare acciones de significación sexual ante una persona menor de catorce

años, la hiciere ver o escuchar material pornográfico o presenciar espectáculos del mismo carácter, será castigado con presidio menor en su grado medio a máximo.

Si, para el mismo fin de procurar su excitación sexual o la excitación sexual de otro, determinare a una persona menor de catorce años a realizar acciones de significación sexual delante suyo o de otro, la pena será presidio menor en su grado máximo.

Con iguales penas se sancionará a quien realice alguna de las conductas descritas en los incisos anteriores con una persona menor de edad pero mayor de catorce años, concurriendo cualquiera de las circunstancias del numerando 1º del artículo 361 o de las enumeradas en el artículo 363.".

"Artículo 30.- La participación en la producción de material pornográfico en cuya elaboración hayan sido utilizados menores de dieciocho años y la comercialización, importación, exportación, distribución o exhibición de ese material, serán sancionadas de conformidad a lo previsto en los artículos 366quinquies, 374 bis y 374 ter del Código Penal."[63].

Descargar Documento completo en:

http://www.leychile.cl/Consulta/listaresultadosavanzada?stringBusqueda=3%23normal%2319927%7C%7C117%23normal%23on%7C%7C48%23normal%23on&tipoNormaBA=&o=experta

ANEXO H. Legislación Delitos Informáticos en Ecuador

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS (Ley No. 67 del 27 de Febrero de 2002)

Art. 3.- Incorporación por remisión.- Se reconoce validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que figure en el

[63]Ministerio de Justicia (2003). *Ley 19927Modifica el código penal, el código de procedimiento penal yel código procesal penal en materia de delitos depornografía infantil.* Chile. Biblioteca del Congreso Nacional.

mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes.

Art. 4.- Propiedad Intelectual.- Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual.

Art. 5.- Confidencialidad y reserva.- Se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención. Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional.

Art. 6.- Información escrita.- Cuando la Ley requiera u obligue que la información conste por escrito, este requisito quedará cumplido con un mensaje de datos, siempre que la información que éste contenga sea accesible para su posterior consulta.

Art. 7.- Información original.- Cuando la Ley requiera u obligue que la información sea presentada o conservada en su forma original, este requisito quedará cumplido con un mensaje de datos, si siendo requerido conforme a la Ley, puede comprobarse que ha conservado la integridad de la información, a partir del momento en que se generó por primera vez en su forma definitiva, como mensaje de datos.

Art. 9.- Protección de datos.- Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

Art. 10.- Procedencia e identidad de un mensaje de datos.- Salvo prueba en contrario se entenderá que un mensaje de datos proviene de quien lo envía y, autoriza a quien lo recibe, para actuar conforme al contenido del mismo, cuando de su verificación exista concordancia entre la identificación del emisor y su firma electrónica.

Art. 11.- Envío y recepción de los mensajes de datos.- Salvo pacto en contrario, se presumirá que el tiempo y lugar de emisión y recepción del mensaje de datos

Art. 12.- Duplicación del mensaje de datos.

Art. 13.- Firma electrónica.- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan

ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

Art. 16.- La firma electrónica en un mensaje de datos.- Cuando se fijare la firma electrónica en un mensaje de datos, aquélla deberá enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste.

Art. 32.- Protección de datos por parte de las entidades de certificación de información acreditadas.- Las entidades de certificación de información garantizarán la protección de los datos personales obtenidos en función de sus actividades, de conformidad con lo establecido en el artículo 9 de esta ley.

Art. 33.- Prestación de servicios de certificación por parte de terceros.- Los servicios de certificación de información podrán ser proporcionados y administrados en todo o en parte por terceros. Para efectuar la prestación, éstos deberán demostrar su vinculación con la Entidad de Certificación de Información.

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Art. 58.- A continuación del Art. 202, inclúyanse los siguientes artículos in numerados:

"Art. ....- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales, la pena será de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales, será sancionada con pena de reclusión menor ordinaria de tres a seis años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Si la divulgación o la utilización fraudulenta se realiza por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena de reclusión menor de seis a nueve años y multa de dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Art. .- Obtención y utilización no autorizada de información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.".

Art. 59.- Sustitúyase el Art. 262 por el siguiente:

"Art. 262.- Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo.".

Art. 60.- A continuación del Art. 353, agréguese el siguiente artículo in numerado:

"Art. ....- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alterno modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;

2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;

3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este capítulo.".

Art. 61.- A continuación del Art. 415 del Código Penal, inclúyanse los siguientes artículos in numerados:

"Art. ....- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

La pena de prisión será de tres a cinco años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculada con la defensa nacional.

Art. ....- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica.".

Art. 62.- A continuación del Art. 553, añadan se los siguientes artículos in numerados:

"Art. ....- Apropiación ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizar en fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Art. ....- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios

1. Inutilización de sistemas de alarma o guarda;

2. Descubrimiento descifrado de claves secretas o encriptadas;

3. Utilización de tarjetas magnéticas o perforadas;

4. Utilización de controles o instrumentos de apertura a distancia; y,

5. Violación de seguridades electrónicas, informáticas u otras semejantes.".

Art. 63.- Añádase como segundo inciso del artículo 563 del Código Penal, el siguiente:

"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito, utilizando medios electrónicos o telemáticos.".

Art. 64.- A continuación del numeral 19 del artículo 606 añádase el siguiente:

"..... Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos."[64].

Descargar Documento completo en:

http://www.redipd.org/legislacion/common/legislacion/ecuador/ecuador_ley_2002-67_17042002_comelectronico.pdf

ANEXO I. Legislación Delitos Informáticos en Perú

LEY Nº 30096 del 22 de Octubre de 2013

LEY DE DELITOS INFORMÁTICOS

Artículo 2. Acceso ilícito

El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.

Artículo 3. Atentado contra la integridad de datos informáticos

[64]Ley No. 2002-67, *Registro Oficial* 557-S § Ecu (2002).

El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

Artículo 4. Atentado contra la integridad de sistemas informáticos

El que, a través de las tecnologías de la información o de la comunicación, inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa.

Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos

El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal.

Artículo 6. Tráfico ilegal de datos

El que crea, ingresa o utiliza indebidamente una base de datos sobre una persona natural o jurídica, identificada o identificable, para comercializar, traficar, vender, promover, favorecer o facilitar información relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga, creando o no perjuicio, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

Artículo 7. Interceptación de datos informáticos

El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático

que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.

Artículo 8. Fraude informático

El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.

La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.

Artículo 9. Suplantación de identidad

El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años.

Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.

“Artículo 1. Marco y finalidad

La presente Ley tiene por finalidad desarrollar legislativamente la facultad constitucional otorgada a los jueces para conocer y controlar las comunicaciones de las personas que son materia de investigación preliminar o jurisdiccional.

Solo podrá hacerse uso de la facultad prevista en la presente Ley en los siguientes delitos:

1. Secuestro.
2. Trata de personas.
3. Pornografía infantil.
4. Robo agravado.
5. Extorsión.
6. Tráfico ilícito de drogas.
7. Tráfico ilícito de migrantes.
8. Delitos contra la humanidad.
9. Atentados contra la seguridad nacional y traición a la patria.
10. Peculado.
11. Corrupción de funcionarios.
12. Terrorismo.
13. Delitos tributarios y aduaneros.
14. Lavado de activos.
15. Delitos informáticos.”

SEGUNDA. Modificación de la Ley 30077, Ley contra el crimen organizado

Artículo 230. Intervención o grabación o registro de comunicaciones telefónicas o de otras formas de comunicación

Artículo 235. Levantamiento del secreto bancario

5. Las empresas o entidades requeridas con la orden judicial deberán proporcionar, en el plazo máximo de treinta días hábiles, la información correspondiente o las actas y documentos, incluso su original, si así se ordena, y todo otro vínculo al proceso que determine por razón de su actividad, bajo apercibimiento de las responsabilidades establecidas en la ley. El juez fija el plazo en atención a las características, complejidad y circunstancias del caso en particular.

“Artículo 162. Interferencia telefónica

El que, indebidamente, interfiere o escucha una conversación telefónica o similar será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al artículo 36, incisos 1, 2 y 4.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia.

La pena privativa de libertad será no menor de ocho ni mayor de diez años cuando el delito comprometa la defensa, la seguridad o la soberanía nacionales.

Artículo 183-A. Pornografía infantil

El que posee, promueve, fabrica, distribuye, exhibe, ofrece, comercializa o publica, importa o exporta por cualquier medio objetos, libros, escritos, imágenes, videos o audios, o realiza espectáculos en vivo de carácter pornográfico, en los cuales se utilice a personas de catorce y menos de dieciocho años de edad, será sancionado con pena privativa de libertad no menor de seis ni mayor de diez años y con ciento veinte a trescientos sesenta y cinco días multa.

La pena privativa de libertad será no menor de diez ni mayor de doce años y de cincuenta a trescientos sesenta y cinco días multa cuando:

1. El menor tenga menos de catorce años de edad.

2. El material pornográfico se difunda a través de las tecnologías de la información o de la comunicación.[65]

Descargar Documento completo en:

http://www2.congreso.gob.pe/Sicr/TraDocEstProc/Contdoc02_2011_2.nsf/d99575da99ebfbe305256f2e006d1cf0/a8851de57eec4e8205257c0c004fc83d/$FILE/30096.pdf

[65] Normas Legales – El Peruano. (2013). *Ley No. 30096 – Ley de Delitos Informáticos.* Perú. Congreso de la República.

ANEXO J. LEY Nº 30171 del 06 de Marzo de 2014.

LEY QUE MODIFICA LA LEY 30096, LEY DE DELITOS INFORMÁTICOS

Artículo 1. Modificación de los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096, Ley de Delitos Informáticos

Modificase los artículos 2, 3, 4, 5, 7, 8 y 10 de la Ley 30096, Ley de Delitos Informáticos, en los siguientes términos:

“Artículo 2. Acceso ilícito

El que deliberada e ilegítimamente accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.

Será reprimido con la misma pena, el que accede a un sistema informático excediendo lo autorizado.”

“Artículo 3. Atentado a la integridad de datos informáticos

El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.”

“Artículo 4. Atentado a la integridad de sistemas informáticos

El que deliberada e ilegítimamente inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.”

“Artículo 5. Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos. El que a través de internet u otro medio análogo contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la

pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal."

"Artículo 7. Interceptación de datos informáticos El que deliberada e ilegítimamente intercepta datos informáticos en transmisiones no públicas, dirigidos a un sistema informático, originados en un sistema informático o efectuado dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con una pena privativa de libertad no menor de tres ni mayor de seis años. La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública. La pena privativa de libertad será no menor de ocho ni mayor de diez cuando el delito comprometa la defensa, seguridad o soberanía nacionales. Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores."

"Artículo 8. Fraude informático El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días-multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social."

"Artículo 10. Abuso de mecanismos y dispositivos informáticos

El que deliberada e ilegítimamente fabrica, diseña, desarrolla, vende, facilita, distribuye, importa u obtiene para su utilización, uno o más mecanismos, programas informáticos, dispositivos, contraseñas, códigos de acceso o cualquier otro dato informático, específicamente diseñados para la comisión de los delitos previstos en la presente Ley, o el que ofrece o presta servicio que contribuya a ese propósito, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa."

Artículo 3. Incorporación del artículo 12 a la Ley 30096, Ley de Delitos Informáticos

Incorpórase el artículo 12 a la Ley 30096, Ley de Delitos Informáticos, en los siguientes términos:

“Artículo 12. Exención de responsabilidad penal Está exento de responsabilidad penal el que realiza las conductas descritas en los artículos 2, 3, 4 y 10 con el propósito de llevar a cabo pruebas autorizadas u otros procedimientos autorizados destinados a proteger sistemas informáticos.”

“Artículo 162. Interferencia telefónica. El que, indebidamente, interfiere o escucha una conversación telefónica o similar, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años.

Si el agente es funcionario público, la pena privativa de libertad será no menor de cuatro ni mayor de ocho años e inhabilitación conforme al artículo 36, incisos 1, 2 y 4.

La pena privativa de libertad será no menor de cinco ni mayor de ocho años cuando el delito recaiga sobreinformación clasificada como secreta, reservada o confidencial de conformidad con la Ley 27806, Ley de Transparencia y Acceso a la Información Pública. La pena privativa de libertad será no menor de ocho ni mayor de diez años, cuando el delito comprometa la defensa, seguridad o soberanía nacionales.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en los supuestos anteriores.”

“Artículo 154-A. Tráfico ilegal de datos personales El que ilegítimamente comercializa o vende información no pública relativa a cualquier ámbito de la esfera personal, familiar, patrimonial, laboral, financiera u otro de naturaleza análoga sobre una persona natural, será reprimido con pena privativa de libertad no menor de dos ni mayor de cinco años.

Si el agente comete el delito como integrante de una organización criminal, la pena se incrementa hasta en un tercio por encima del máximo legal previsto en el párrafo anterior.”

“Artículo 183-B. Proposiciones sexuales a niños, niñas y adolescentes

El que contacta con un menor de catorce años para solicitar u obtener de él material pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho

años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36. Cuando la víctima tiene entre catorce y menos de dieciocho años de edad y medie engaño, la pena será no menor de tres ni mayor de seis años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36."

"Artículo 230. Intervención, grabación o registro de comunicaciones telefónicas o de otras formas de comunicación y geo localización de teléfonos móviles

(…)

4. Los concesionarios de servicios públicos de telecomunicaciones deben facilitar, en forma inmediata, la geo localización de teléfonos móviles y la diligencia de intervención, grabación o registro de las comunicaciones que haya sido dispuesta mediante resolución judicial, en tiempo real y en forma ininterrumpida, las 24 horas de los 365 días del año, bajo apercibimiento de ser pasible de las responsabilidades de Ley en caso de incumplimiento. Los servidores de las indicadas empresas deben guardar secreto acerca de las mismas, salvo que se les citare como testigo al procedimiento. Dichos concesionarios otorgarán el acceso, la compatibilidad y conexión de su tecnología con el Sistema de Intervención y Control de las Comunicaciones de la Policía Nacional del Perú. Asimismo, cuando por razones de innovación tecnológica los concesionarios renueven sus equipos y software, se encontrarán obligados a mantener la compatibilidad con el sistema de intervención y control de las comunicaciones de la Policía Nacional del Perú. (…)."[66]

Descargar Documento completo en:

http://www2.congreso.gob.pe/Sicr/TraDocEstProc/Contdoc02_2011_2.nsf/d99575da99ebfbe305256f2e006d1cf0/e0589bd1613de56e05257c97004d0f7a/$FILE/30171.pdf

[66] Normas Legales – El Peruano. (2014). *Ley No. 30171 – Ley que Modifica La Ley 30096, Ley de Delitos Informáticos.* Perú. Congreso de la República

ANEXO K. Legislación Delitos Informáticos en Venezuela

Ley Especial Contra los Delitos Informáticos (Gaceta Oficial del 30 de Octubre de 2001).

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 sujeto 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 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. El 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. El que destruya, dañe, modifique o realice cualquier acto que altere el funcionamiento o inutilice un sistema que utilice tecnologías de información o cualquiera 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 cualquiera 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, por cualquier medio, de un virus o programa análogo.

Artículo 8.-

Sabotaje o daño culposos. 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 cualquiera 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. El que, con el propósito de destinarlos a vulnerar o eliminar la seguridad de cualquier sistema que utilice tecnologías de información, importe, fabrique, posea, distribuya, venda o utilice equipos, dispositivos o programas; 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. El que indebidamente obtenga, revele o difunda la data o información contenidas en un sistema que utilice tecnologías de información o en cualquiera de sus componentes, será penado con prisión de cuatro a ocho años y multa de cuatrocientas a ochocientas 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. El que, 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. El que 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. El 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. El que, 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. El 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 el 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 penado 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. El que se apropie de una tarjeta inteligente o instrumento destinado a los mismos fines, que se hayan perdido, extraviado o hayan sido entregados por equivocación, con el fin de retenerlos, usarlos, venderlos o transferirlos a 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. El 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. El 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. El que por cualquier medio se apodere, utilice, modifique o elimine, 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 penado 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. El 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 sancionado 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. El que 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 precedentes, aun cuando el autor no hubiese tomado parte en la comisión de dichos delitos, 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. El 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. El 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 penado 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. El que 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. El 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 sancionado 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:

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

2º 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 accesorias siguientes:

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

2º 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.

3º 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 públicos, del ejercicio privado de una profesión u oficio o del desempeño en una institución o empresa privadas, respectivamente.

4º 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 disponer, además, 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. [67]

Descargar Documento completo en:

http://www.tsj.gov.ve/legislacion/LeyesEspeciales/3.-GO_37313.pdf

[67]Ley Especial Contra los Delitos Informáticos, Ven. § (2001).