UNIVERSIDAD MAYOR DE SAN ANDRÉS

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

CARRERA DE DERECHO

PETAENG

MONOGRAFIA-PETAENG

“NECESIDAD DE AMPLIAR LA PENALIZACIÓN DE LOS DELITOS INFORMATICOS EN BOLIVIA REFERENTES A ESTAFA ELECTRONICA”

(Monografía para optar al grado de Licenciatura en Derecho)

POSTULANTE: **Giovana Elizabeth Avilés Ávalos**

TUTORA : **Dra. Karina Medinaceli**

La Paz-Bolivia

2014

DEDICATORIA

Dedico este trabajo a Dios por haberme dado sabiduría y las fuerzas necesarias para seguir adelante.

A mis padres por ser el pilar más importante de mi vida, por estar a mi lado y por darme su apoyo, cariño y comprensión

AGRADECIMIENTOS

A todas las personas que siempre me colaboraron de una u otra manera, especialmente a la Dra. Karina Medinacelli por brindarme su apoyo incondicional en la realización del presente trabajo.

RESUMEN

Junto al creciente y significativo avance que ha generado el desarrollo, difusión y uso de la informática y su influencia dentro de la actividad cotidiana a nivel mundial, surgen nuevos comportamientos ilícitos que van en contra de la sociedad y que en su momento son denominados "Delitos Informáticos". Como consecuencia de este avance tecnológico podemos observar un incremento de conductas antijurídicas tales como la "Estafa Electrónica", lo que implica responsabilidad para aquellas personas que las cometen y a la ausencia de una ley aplicable a este tipo de delitos dentro de nuestra sociedad se hace necesaria una correcta tipificación y penalización en Bolivia.

La legislación boliviana debe adecuarse a los cambios y a la evolución de la sociedad para de esta manera poder realizar un correcto tratamiento de las distintas formas antijurídicas informáticas. Es imperativo que la Tecnología de la Información y Comunicación sea regulada de forma tal que no exista tanta inexactitud dentro del ámbito jurídico y, de esta manera exista un mejoramiento en cuestiones de seguridad informática, no solamente al referirnos a la parte técnica, sino también a las consecuencias que pueden llevar consigo la violación de las mismas dentro del ámbito jurídico.

El desarrollo de la presente investigación tiene por objeto el análisis de los delitos informáticos relacionados con "Estafa Electrónica" y demostrar la necesidad que existe para ampliar o modificar su penalización dentro de nuestro ordenamiento jurídico previo estudio de los delitos informáticos, su conceptualización, generalidades asociadas al fenómeno y el papel que juega el Estado Boliviano frente al surgimiento de estas nuevas figuras delictivas. Es importante también el análisis crítico del Ordenamiento Penal Boliviano y su estudio comprado con legislaciones de diferentes países, especialmente latinoamericanos para así poder observar posibles falencias y soluciones y, de esta manera poder proponer un Proyecto de Normativa que ayudará a tal efecto.

INDICE

CAPITULO II

DELITOS INFORMATICOS

CAPITULO III

ESTAFA ELECTRÓNICA

INTRODUCCIÓN

En la actualidad, la Informática esta presente en todos los campos de la vida cotidiana ya sea a nivel laboral como recreacional, esto permite poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance de millones de interesados y de usuarios. De esta manera, la Informática se convierte en una de las fuerzas más poderosas de la sociedad actual.

Las redes de comunicación electrónica y los sistemas de información forman parte integrante de la vida diaria de los ciudadanos en el mundo y desempeñan un papel fundamental en el éxito de la economía universal. Cada vez están más interconectadas y es mayor la convergencia de los sistemas de información y las redes.

Así como la actividad informática crece a pasos inconmensurables, a través de esta, la actividad delictiva manifestada de formas inimaginables va creciendo a nivel global. El incremento de la delincuencia informática encuentra respuestas en una variedad de factores así como la tecnología disponible tanto para el delincuente como para las víctimas, combinado con el escaso conocimiento de quienes y cómo deben protegerse de estos delitos que se incrementan a través de la nueva tecnología, facilitando de esta manera la afectación de bienes jurídicamente protegidos como la intimidad, el orden socioeconómico, la fe pública y la seguridad del Estado, entre otros.

Surgen diferentes tipos de delitos informáticos como ser la piratería informática, el terrorismo informático, el sabotaje informático, entre otros; siendo uno de los más comunes el denominado "Estafa Electrónica o Fraude Informático" existiendo diversas modalidades para su comisión, sea en el ingreso y/o salida de datos, modificación de programas existentes; incrementándose dicha conducta día a día y siendo necesaria una correcta regulación debido a que nuestra sociedad no esta exenta de este tipo de actividades delincuenciales cometidas a través del ciberespacio.

La criminalidad informática como fenómeno de la era tecnológica se caracteriza por su carácter transnacional, dificultad de descubrimiento e impunidad, esto debido a la falta de protección jurídica idónea a la realidad social y tecnológica en que vivimos, sumando el carácter especial de las conductas que no admiten encuadrarse dentro de las figuras tradicionales, siendo necesaria la creación de nuevas figuras delincuenciales dentro de nuestro ordenamiento jurídico penal.

En este marco, la presente investigación tiene por objeto analizar la situación de los delitos informáticos referentes a "Estafa Electrónica" y demostrar la necesidad de ampliar su penalización dentro de nuestro ordenamiento jurídico, previo análisis de los delitos informáticos en general, ya que a partir de esto se pueden aclarar aspectos tales como: sujetos, elementos, bienes jurídicos que se protegen, características, clases y posibles modos de prevención.

Analizar de manera crítica el Ordenamiento Jurídico Penal Boliviana con referencia a los delitos informáticos, sus posibles falencias y posibles soluciones que deben ser tomadas en cuenta para evitar que este tipo de delitos alcancen los niveles de peligrosidad que se dan en otros países.

Finalmente, con la necesidad de ampliar la penalización de los delitos informáticos en Bolivia referentes a "Estafa Electrónica", se realizará un estudio acerca del derecho comparado de diferentes países de Latinoamérica para concluir con un Proyecto de Normativa que ayudará a tal efecto.

Se utilizarán los métodos deductivo y el de investigación documental para realizar un análisis profundo referente al tema de investigación y, para poder realizar el análisis comparativo con legislaciones de diferentes países se utilizará el método lógico jurídico. La interpretación jurídica y la revisión bibliográfica también serán necesarias para el correcto desarrollo del trabajo de investigación.

CAPITULO I
DISEÑO DE INVESTIGACIÓN

1.1. IDENTIFICACIÓN DEL PROBLEMA

Producto de la globalización y del desarrollo de la tecnología informática como una de las fuerzas más poderosas a nivel mundial y su influencia en la sociedad actual debido a que esta se encuentra inmersa en todos los campos de la vida moderna, la red de internet se ha vuelto parte indispensable de la vida cotidiana y trajo muchos beneficios tanto a empresas como a particulares.

El progreso de la informática nos da la posibilidad de procesar y poner a disposición una ingente cantidad de información de diversa naturaleza al alcance de millones de usuarios facilitado por el uso de la red de internet. Debido a esto surgen también nuevas formas o comportamientos antisociales y delictivos que se manifiestan de formas inimaginables y que afectan a un conjunto de bienes jurídicamente protegidos, esto genera la necesidad de prevenir y sancionar este mal uso del internet debido a que no estamos exentos de ese tipo de actividades delincuenciales a raíz del desarrollo tecnológico y el incremento de los delitos informáticos.

Por tanto, cualquier persona puede ser victima de delitos, tanto en el mundo real como en el virtual. Sin embargo, parecería que este tipo de conductas gozan de cierta impunidad, toda vez que la tecnología y la ciencia han avanzado a pasos agigantados y han rebasado al derecho.

El principio de legalidad expresado en la máxima “Nullum crimen nulla poena sine lege” establece que no hay delito ni pena sin ley previa. Esto significa que en el orden penal la ley debe contener la descripción precisa de las acciones delictivas a ser penadas y al existir escasos tipos penales descritos existe impunidad para la gente que comete este tipo de delitos, esto demanda una mayor y más rápida actividad por parte de los legisladores.

La problemática fundamental, debido al incremento de usuarios de la red de internet y a la aparición de nuevas formas delictivas que ocasionan problemas gravísimos tratando de buscar soluciones prontas ya que hoy en día no hay suficientes formas de combatirlas, reside en la urgente necesidad de ampliar y modificar la normativa referida a los delitos informáticos contenida en el Código Penal debido a la existencia de delitos como la estafa electrónica, los daños informáticos, la pornografía infantil, la difusión de mensajes injuriosos y calumniosos y otros vía internet, mismos que merecen un tratamiento especial en nuestro ordenamiento jurídico penal.

1.2. PROBLEMATIZACIÓN

- ¿Por qué existe la necesidad de penalizar la “Estafa Electrónica” en Bolivia?
- ¿Por qué este tipo de delito es impune en Bolivia?
- ¿Qué se debe hacer para disminuir el índice de “Estafa Electrónica” en Bolivia?
- **¿**La globalización ha logrado rebasar nuestro sistema jurídico?
- ¿Que se propone para dar solución a este tipo de problemática social?

1.3. DELIMITACIÓN DEL TEMA

1.3.1. Delimitación Temática

La presente investigación se encuentra orientada al estudio de posibles modificaciones y/o ampliaciones en nuestro ordenamiento jurídico penal, concretamente en el título XII (Delitos contra la Propiedad) en su capítulo XI, artículos 363 bis y 363 ter (Delitos Informáticos) en lo que corresponde a "Estafa Electrónica".

1.3.2. Delimitación Temporal

El presente trabajo de investigación tomará como parámetro el año 2011 hasta el presente, debido al desarrollo inconmensurable de la tecnología como principal medio de comunicación y el alto grado de criminalidad que crece a pasos agigantados por el mal uso de esta.

1.3.3. Delimitación espacial

El alcance espacial será a nivel local tomando en cuenta la investigación en la ciudad de La Paz.

1.4. FUNDAMENTACIÓN E IMPORTANCIA DEL TEMA

Como consecuencia del avance tecnológico de la Informática se observa un incremento inconmensurable de conductas antijurídicas tales como la "Estafa Electrónica", misma que implica responsabilidad para aquellos que la cometen y a la ausencia de una ley aplicable a este tipo de delitos denominados "Informáticos" utilizando como instrumento o medio la red de Internet, hace que exista la necesidad de tipificarlos y penalizarlos en Bolivia.

La legislación boliviana debe adecuarse a los cambios y a la evolución de la sociedad para de esta manera poder realizar un correcto tratamiento de las

distintas formas antijurídicas informáticas. Es imperativo que la Tecnología de la Información y Comunicación sea regulada de forma tal que no exista tanta inexactitud dentro del ámbito jurídico y, de esta manera exista un mejoramiento en cuestiones de seguridad informática, no solamente al referirnos a la parte técnica, sino también a las consecuencias que pueden llevar consigo la violación de las mismas dentro del ámbito jurídico.

1.5. OBJETIVOS

1.5.1. Objetivo General

El objetivo de la presente investigación consiste en realizar un análisis científico jurídico de las normas legales vigentes en nuestro actual ordenamiento jurídico penal referentes a delitos informáticos, tendiente a demostrar si la normativa es suficiente o por el contrario existe la necesidad de ampliarla y/o modificarla.

1.5.2. Objetivos Específicos

- Realizar un relevamiento acerca de la legislación Boliviana referida a los delitos informáticos.

- Estudiar el fenómeno como tal y el impacto que tienen estos dentro de cualquier tipo de organización.

- Describir los nuevos delitos informáticos en la legislación comparada.

- Analizar la Estafa Electrónica en nuestro Estado Plurinacional, su peligrosidad y las medidas preventivas que se deben tomar en cuenta con la presencia de este.

1.6. MARCO DE REFERENCIA

1.6.1. Marco Histórico

"El término "Delito Informático" se acuñó a finales de los años noventa, a medida que la red de Internet se expandió por toda Norteamérica. Después de una reunión en Lyon, Francia, se fundo un subgrupo del grupo de naciones que conforman el denominado "G8" con el objetivo de estudiar los problemas emergentes de criminalidad que eran propiciados por o que migraron a Internet. El "Grupo de Lyon" utilizó el término para describir de forma muy imprecisa todos los tipos de delitos perpetrados en la red o en las nuevas redes de telecomunicaciones que tuvieran un rápido descenso en los costos"[1].

Al analizar la legislación boliviana se habla primero de la Ley 1322 de derechos de autor, en la cual se incluye por primera vez el año 1992 la protección estatal a programas de computación o software, cuya reglamentación específica se aprobó recién en 1997 con el D.S. 24582. A partir de este momento una serie de leyes y decretos dispersos norman actividades específicas en el uso de la tecnología hasta la aprobación de la ley 164 de Telecomunicaciones del 8 de agosto de 2011, que representa una de las normas vigentes más completas hasta ahora sobre la regulación de las actividades informáticas. Se incorporan también normas referidas a la creación de instituciones y medidas que fortalecen el uso de la ciencia y la tecnología en el país como política pública porque sientan las bases para la transversalización de la informática en diferentes espacios

[1] http://pcolorador.blogspot.com/2008/04/delitosinformaticos_14htm

públicos y privados. Por ejemplo, se incluye la Ley 2209 de Fomento a la Ciencia, Tecnología e Innovación el año 2001.

El 10 de marzo de 1997, se promulga la Ley 1768 "Ley de Modificaciones al Código Penal", esta Ley, en su numeral 57 dispone la inclusión del capítulo XI dependiente del capítulo XII del libro segundo del Código Penal, referido a los "Delitos Informáticos, incluidos dentro de los artículos 363 Bis y 363 Ter, cuyas tipificaciones son: manipulación informática y alteración, acceso y uso indebido de datos informáticos respectivamente.

Bolivia se encuentra rezagada porque no cuenta con un cuerpo normativo integral y diversificado para todas las áreas que hoy debieran estar reguladas como las diferentes formas de delitos por Internet o las acciones delincuenciales a través de las redes sociales como el Facebook y Twitter.

1.6.2. Marco Teórico

El autor mejicano Julio Téllez Valdez (1995) conceptualiza al delito informático en forma típica y atípica, entendiendo por la primera a "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por las segundas "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"[2]. De esta manera, decimos que los delitos informáticos son conductas ilícitas sancionadas por el Derecho Penal y que para su realización los delincuentes se valen de computadoras como medio o fin para su comisión, estableciendo un medio de cultivo denominado Internet.

[2] Téllez Valdez, Julio. Pg. 163

"Al hablar de Estafa Electrónica hacemos referencia a estafas producidas a través de medios computacionales. No existe en la actualidad una manera definitiva de prevenir totalmente este delito, pero muchos países han votado legislaciones especiales para enfrentarlo"[3].

Para realizar un análisis de este tipo de delitos y debido a la urgente necesidad de regularlos, sancionarlos y prevenirlos, se hará un estudio bajo los principios de la Teoría del Delito y del Positivismo Jurídico, realizando una crítica de cada uno de sus elementos en sus aspectos jurídico, social, económico y político.

1.6.3. Marco Conceptual

Durante el proceso de investigación será necesaria la utilización de conceptos fundamentales que servirán como claves para el correcto desarrollo del mismo:

- **Derecho:** "Es el orden normativo e institucional de la conducta humana en la sociedad inspirada en postulados de justicia y certeza jurídica, cuya base son las relaciones sociales existentes que determinan su contenido y carácter en un momento y lugar dado"[4].

- **Derecho Penal: "**Constituye la espina dorsal de las ciencias penales al determinar que es lo que debe considerarse como delito"[5].

[3] http://www.drleyes.com/page/diccionario_juridico/significado/E/1237/ESTAFAS-ELECTRONICAS/ (consultado 23/11/14)
[4] García Máynez, Eduardo. Pg. 18

[5] Cajias, Huascar. Pg. 32

- **Delito:** "Etimológicamente, la palabra delito proviene del latín delictum, expresión también de un hecho antijurídico y doloso castigado con una pena. En general, culpa, crimen, quebrantamiento de una ley imperativa"[6]**.**

- **Delincuente: "**Es la persona que delinque; el sujeto activo de un delito o falta, como autor, cómplice o encubridor. A estas dos últimas categorías no suele imponérsele penalidad en las faltas. El individuo condenado por un delito o una falta penados. Delincuente es el que, con intención dolosa, hace lo que la ley ordinaria prohíbe u omite, siempre que tal acción u omisión se encuentre penada en la ley"[7].

- **Ley: "**Genéricamente, modo de ser y obrar de los seres. Norma o precepto de la autoridad pública que manda, prohíbe o permite algo. Regla de conducta obligatoria dictada por el Poder Legislativo, o por el ejecutivo cuando lo sustituye o se arroga sus atribuciones"[8]

- **Pena: "**Recurso que utiliza el Estado para reaccionar frente al delito, expresándose como la restricción de derechos del responsable. La pena también se define como una sanción que produce la pérdida o restricción de derechos personales, contemplada en la ley e impuesta por el órgano jurisdiccional, mediante un proceso, al individuo responsable de la comisión de un delito"[9]

[6] Cabanellas de Torrez, Guillermo.

[7] Ibid.

[8] Ibid.

[9] http://es.wikipedia.org/wiki/pena

- **Informática:** Konrad Zuse, citado por Raúl Rojas dice: "La Informática es la disciplina que estudia el tratamiento automático de la información utilizando dispositivos electrónicos y sistemas computacionales. También es definida como el procesamiento de información en forma automática"[10]

- **Derecho Informático: "**Conjunto de principios y normas que regulan los efectos jurídicos de la relación entre el Derecho y la Informática. También se le considera como una rama del Derecho especializada en el tema de la Informática, sus usos, sus aplicaciones y sus implicaciones legales"[11].

- **Delito Informático:** "cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos"[12]

- **Delincuencia o criminalidad Informática:** "Maniobras fraudulentas que puede hacer el ordenador, por medio o por circunstancia, volcando en caso determinado bajo la capa de incriminaciones no específicas a la informática (roles de ficheros, alteraciones en el ordenador, etc.). Otras figuras del delito han sido especialmente creadas para sancionar actos fraudulentos que sólo se producen en ocasión de una operación informática"[13]

---

[10] Rojas Raúl (1998). «How to make Zuse's Z3 a universal computer». *IEEE Annals of the History of Computing* **20**: pp. 51–54. (Consultado 23/11/14)

[11] http://es.wikipedia.org/wiki/derecho_informatico

[12] Correa Carlos. Pg. 295

[13] Azpilcueta, Hermilio Tomás. Pg 61

- **Internet: "**Es el nombre que se le da a una red creada a partir de un proyecto del Departamento de Defensa de Estados Unidos llamado DARPANET, iniciado en 1909 y cuyo propósito principal era la investigación y desarrollo de protocolos de comunicación para redes de área amplia para ligar redes. Podemos definir a Internet como una "red de redes", es decir, una red que no sólo interconecta computadoras, sino que interconecta redes de computadoras entre si. Una red de computadoras es un conjunto de máquinas que se comunican a través de algún medio (cable coaxial, fibra óptica, radiofrecuencia, líneas telefónicas, etc.) con el objeto de compartir recursos"[14].

- **Actividad Ilícita:** "Actos contrarios a las buenas costumbres o prohibidos por las leyes y que son reprobables ante la sociedad"[15].

- **Estafa:** "acción de obtener para sí o un tercero un beneficio económico indebido, mediante engaños o artificios, provoque o fortalezca error en otro que motive la realización de un acto de disposición patrimonial en perjuicio del sujeto en error o de un tercero"[16]

  Estafa Electrónica: "Manipulación informática o artificio similar que concurriendo ánimo de lucro, consiga una transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero"[17]

[14] http://www.cad.com.mx/que_es_internet.htm

[15] www.perucontable.com

[16] Código Penal Bolviano. Art. 335

[17] Ribas Alejandro, Javier. Pg. 128

- **Manipulación Informática:** "Interacción persona-computador que incluye la continua representación de los objetos de interés y acciones. Operar con las manos o con un instrumento el computador, intervenir con medios hábiles para distorsionar la realidad al servicio de intereses particulares".[18]

1.6.4. Marco Jurídico

A nadie escapa la enorme influencia que ha alcanzado la informática en la vida diaria de las personas y organizaciones, además de la importancia que tiene su progreso para el desarrollo de un país. Las transacciones comerciales, la comunicación, los procesos industriales, las investigaciones, la seguridad, etc., son todos aspectos que dependen cada día más de un adecuado desarrollo de la tecnología informática. Junto al avance de la tecnología informática y su influencia en casi todas las áreas de la vida social, surge una serie de comportamientos ilícitos conocidos como "delitos informáticos" y que necesitan de una correcta regularización.

- **CONSTITUCIÓN POLÍTICA DEL ESTADO PLURINACIONAL DE BOLIVIA**

La CPE Plurinacional de Bolivia, aprobada en enero de 2009, en su Capítulo dedicado a los Derechos Civiles y Políticos, establece en el artículo 21, numeral 2 que:

Las bolivianas y los bolivianos tienen los siguientes derechos: " A la privacidad, intimidad, honra, honor, propia imagen y dignidad"[19].

[18] es.wikipedia.org/wiki/manipulación

[19] Constitución Política del Estado Plurinacional de Bolivia

En el mismo capítulo, el artículo 25 establece:

I. “Toda persona tiene derecho a la inviolabilidad de su domicilio y al secreto de las comunicaciones privadas en todas sus formas, salvo autorización judicial.

II. Son inviolables la correspondencia, los papeles privados y las manifestaciones privadas contenidas en cualquier soporte, éstos no podrán ser incautados salvo en los casos determinados por la ley para la investigación penal, en virtud de orden escrita y motivada de autoridad judicial competente.

III. Ni la autoridad pública, ni persona u organismo alguno podrán interceptar conversaciones o comunicaciones privadas mediante instalación que las controle o centralice.

IV. La información y prueba obtenidas con violación de correspondencia y comunicaciones en cualquiera de sus formas no producirán efecto legal”[20].

En el capítulo sexto dedicado a Educación, Interculturalidad y derechos culturales, en su sección IV, dedicado a Ciencia, Tecnología e Investigación, establece en el artículo 103 que:

I. “El Estado garantizará el desarrollo de la ciencia y la investigación científica, técnica y tecnológica en beneficio del interés general. Se destinarán los recursos necesarios y se creará el sistema estatal de ciencia y tecnología.

[20] Ibid.

II. El Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación.

III. El Estado, las universidades, las empresas productivas y de servicio públicas y privadas y las naciones y pueblos indígena originario campesinos, desarrollarán y coordinaran procesos de investigación, innovación, promoción, divulgación, aplicación y transferencia de ciencia y tecnología para fortalecer la base productiva e impulsar el desarrollo integral de la sociedad, de acuerdo con la ley"[21].

En el capítulo séptimo referido a comunicación social, el artículo 106 establece lo siguiente:

I. "El Estado garantiza el derecho a la comunicación y el derecho a la información.

II. El Estado garantiza a las bolivianas y los bolivianos el derecho a la libertad de expresión, de opinión y de información a la rectificación y a la réplica, y el derecho a emitir libremente las ideas por cualquier medio de difusión, sin censura previa.

III. El Estado garantiza a las trabajadoras y los trabajadores de la prensa, la libertad de expresión, el derecho a la comunicación y a la información.

[21] Constitución Politica del Estado Plurinacional de Bolivia

IV. Se reconoce la cláusula de conciencia de los trabajadores de la información"[22].

Por último, en el Título Cuarto: Garantías Jurisdiccionales y Acciones de Defensa, Capítulo Segundo, Sección III referente a Acción de Protección de Privacidad, el artículo 130 establece lo siguiente:

I. "Toda persona individual o colectiva que crea estar indebida o ilegalmente impedida de conocer, objetar u obtener la eliminación o rectificación de los datos registrados por cualquier medio físico, electrónico, magnético o informático, en archivos o bancos de datos públicos o privados, o que afecten a su derecho fundamental a la intimidad y privacidad personal o familiar, o a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

II. La Acción de Protección de Privacidad no procederá para levantar el secreto en materia de prensa."[23]

Nuestra Carta Magna ha previsto las garantías referidas a los derechos civiles y políticos de todos los ciudadanos, pese a esto, se observa la creciente inseguridad en nuestro país debido a la escasa normativa referente a delitos informáticos. Por esta razón, muchos de estos delitos son tratados como delitos comunes y se incrementan día a día debido a la facilidad que se tiene para cometerlos y a su difícil descubrimiento.

- **CÓDIGO PENAL BOLIVIANO**

  En el tema de legislación de los delitos informáticos en Bolivia, nuestro Código Penal solo tipifica dos de ellos: la Manipulación

[22] Constitución Pólítica del Estado Plurinacional de Bolivia

[23] Ibid.

Informática y la Alteración, Acceso y uso Indebido de Datos Informáticos, lo lamentable es que en el segundo caso no se tiene cárcel. Sin embargo de estas debilidades en la legislación boliviana, cabe mencionar que cuando se cometen estos delitos, casi siempre van de la mano de otros delitos antiguos ya tipificados en el Código Penal. Por ejemplo cuando se realiza la manipulación de los datos (mediante phishing se captura datos de un cliente de un banco) en el proceso de entrada de datos, esta información se utiliza para sacar dinero de esa cuenta que puede ser vía caja, transferencia, cajeros automáticos (ATM), entonces el delito informático (digital) se concreta en algo físico tipificado como Robo. Así como el caso comentado, estos dos delitos (manipulación y acceso indebido) se pueden vincular con otros, como son el robo, hurto, uso de instrumento falsificado, abuso de confianza y otros.

Los delitos citados anteriormente son descritos en el Código Penal de la siguiente manera:

CAPÍTULO XI. DELITOS INFORMÁTICOS

Artículo 363 Bis.- (MANIPULACIÓN INFORMÁTICA). "El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días"[24].

[24] Código Penal Boliviano

Artículo 363 Ter.- (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS). "El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días"[25].

En el capítulo IV que hace referencia a las estafas y otras defraudaciones, el artículo 335 establece:

"El que con la intención de obtener para sí o un tercero un beneficio económico indebido, mediante engaños o artificios provoque o fortalezca error en otro que motive la realización de un acto de disposición patrimonial en perjuicio del sujeto en error o de un tercero, será sancionado con reclusión de uno (1) a cinco (5) años y con multa de sesenta (60) a doscientos (200) días"[26].

Si bien nuestro ordenamiento jurídico penal sanciona algunos delitos informáticos, estos se encuentran algo resagados debido al constante avance de la tecnología, es por esta razón que no existe una tipificación apropiada, amplia y precisa en lo que se refiere a los llamados nuevos delitos informáticos como es la "Estafa Electrónica"

1.7. MÉTODOS A UTILIZAR

1.7.1. Métodos Generales

1.7.1.1. Método deductivo

En la presente investigación se utilizará el método deductivo ya que mediante este se podrán dar conceptos, definiciones, leyes y normas

[25] Ibid.

[26] Ibid

generales referentes a la “Estafa Electrónica” como delito informático y por medio de estas se emitirán conclusiones.

1.7.1.2. Método de la Investigación Documental

Se utilizarán diferentes tipos de documentos para realizar un análisis exhaustivo referente al tema de investigación con la finalidad de obtener resultados.

1.7.1.3. Método Lógico Jurídico

Este método será fundamental para realizar un análisis comparativo con legislaciones de diferentes países.

1.7.2. Métodos Específicos

1.7.2.1 Interpretación Jurídica

El análisis del significado o alcance de las normas legales existentes respecto a delitos informáticos en nuestro país será necesario para llegar a conclusiones sólidas.

1.7.2.2 Revisión Bibliográfica

Se tomará en cuenta la bibliografía necesaria para la realización del trabajo de investigación.

CAPITULO II
DELITOS INFORMÁTICOS

2.1. CONCEPTO

Para referirnos a los delitos como acciones tipificadas en textos jurídico-penales, es necesario tener una noción clara y precisa del significado de la expresión "delitos informáticos". Por este motivo se analizarán conceptos de diferentes autores.

Según Julio Tellez Valdes "los delitos informáticos son actitudes contrarias a los intereses de las personas en que se tiene a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas o culpables en que se tiene a las computadoras como instrumento o fin (concepto típico)"[1].

También se puede definir a los delitos informáticos como "toda conducta ilícita, sancionada por el Derecho Penal, para la realización de las cuales se utilizan los medios informáticos, frutos de las nuevas tecnologías, ya sea como herramienta para la comisión del delito o como fin en sí mismo, afectando los datos contenidos en un sistema o la transmisión de los mismos"[2].

Carlos Correa hace referencia a una definición abarcante de la Organización para la Cooperación Económica y el Desarrollo y dice: "delito informático (computer

[1] Tellez Valdez, Julio. Pg. 163

[2] Viega María José. Pg. 179

crime) es "cualquier conducta, no ética, o no autorizada que involucra el procesamiento automático de datos y/o la transmisión de datos"[3].

Los delitos informáticos son definidos por la doctrina española como "aquellas conductas que ponen en peligro o lesionan la integridad, confidencialidad y/o disponibilidad de los datos y sistemas informáticos, sin perjuicio de que además puedan suponer una puesta en peligro o lesión de bienes jurídicos distintos, también como la realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático, ya sea hardware o software"[4].

Según Ricardo Posada Maya "los delitos informáticos propiamente dichos se relacionan con aquellas conductas lesivas no consentidas, cuyos objetos materiales exclusivos son la confiabilidad (calidad, idoneidad y corrección), la integridad y la disponibilidad de datos o información, y de los componentes lógicos de programación de los equipos informáticos que permiten el tratamiento, transmisión o almacenamiento de los mismos (programas operativos o aplicativos, o software). Objetos que resultan lesionados o puestos en peligro por conductas que los manipulen con fines ilícitos o de lucro, o también por el uso de programas lesivos creados con tal propósito"[5].

De acuerdo con las anteriores definiciones para que exista un delito de esta categoría es imprescindible la utilización de un elemento informático en la comisión de un hecho punible o que el resultado de la acción se traduzca en una vulneración a un sistema informático.

[3] Correa, Carlos. Pg. 295-296

[4] Rico Carrillo, Mariliana. Pg. 209-210

[5] Posada Maya, Ricardo. Pg. 19

2.2. CARACTERÍSTICAS DE LOS DELITOS INFORMÁTICOS

Para la comisión de este tipo de actividades ilícitas se hace necesaria la utilización de medios informáticos y tener características especiales para que de esta manera este tipo de delitos no sean descubiertos fácilmente o sean imposibles de descubrir.

A continuación se citan las siguientes características según Julio Tellez Valdes:

- "Son conductas delictivas de cuello blanco (white collar crimes), término introducido por primera vez por el criminólogo estadounidense Edwin Sutherland al año 1943, en tanto que solo determinado número de personas con ciertos conocimientos (en este caso técnicos) pueden llegar a cometerlas.
- Son acciones ocupacionales porque muchas veces se realizan cuando el sujeto esta en el trabajo.
- Son acciones de oportunidad debido a que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
- Provocan serias pérdidas económicas para los afectados y casi siempre producen beneficios de más de cinco cifras a aquellos que los realizan.
- Ofrecen facilidades de tiempo y espacio, ya que en milésimas de segundo y sin la necesaria presencia física pueden llegar a cometerse.
- Son muchos los casos y pocas las denuncias, todo ello debido a la falta misma de regulación jurídica a nivel internacional.
- Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

- En su mayoría son dolosos o intencionales, aunque también hay muchos de carácter culposo o imprudenciales y en ocasiones van más allá de la intención (preterintencionales).
- Ofrecen facilidades para su comisión a los menores de edad.
- Tienden a proliferar cada vez más, por lo que requieren una urgente regulación jurídica a nivel internacional.
- Por un lado el progreso tecnológico hace más difícil descubrir su comisión, y por otra parte la relativa falta de seguridad de los sistemas y la renuncia a denunciarlos por temor a dañar la imagen ante la clientela, u otros motivos contribuyen a la impunidad."[6]

2.3. BIEN JURÍDICO TUTELADO EN LOS DELITOS INFORMÁTICOS

No debemos olvidarnos del bien jurídicamente protegido o tutelado ya que este es la razón de ser del delito. Este bien lesionado generalmente no esta mencionado en los tipos penales.

Existen varios criterios acerca de cual es el bien jurídico protegido, como por ejemplo:

"El bien jurídico tutelado mediante la sanción de los delitos es la pureza de la técnica que presupone la informática y el resguardo de los medios involucrados en la computación electrónica"[7]

[6] Tellez Valdes, Julio. Pg. 163

[7] Gustavino, Elias. Pg. 82

Algunos autores dicen que existe un bien jurídico nuevo, estrictamente informático, que es objeto de lesión o puesta en peligro en todos los delitos informáticos. "Este nuevo bien jurídico es la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos"[8].

"En general, los bienes jurídicamente tutelados varían según el tipo de delito. Tomando en consideración las tres posibilidades que tienen los sistemas informáticos de incidir en las conductas delictivas, como fin, como medio de comisión o como medio de almacenamiento de pruebas; en el primer caso, es decir, como fin, los bienes jurídicos protegidos son principalmente el patrimonio, la intimidad, aunque puede también ser la economía y la seguridad nacional, si se atacan los sistemas informáticos que manejan la infraestructura crítica y hacen posible el ejercicio del derecho a la información"[9].

"En el segundo caso, cuando se utiliza el sistema informático como medio de comisión, también pueden incluirse dentro de los bienes jurídicos a tutelar, el patrimonio, la intimidad, la seguridad nacional, el honor, la salud, el sano desarrollo psicosexual, y todos los demás bienes jurídicos protegidos por la legislación penal"[10].

"Con relación al tercer caso, la utilización de los sistemas informáticos como medio para almacenar pruebas no resulta del todo exacto hablar de un análisis respecto del bien jurídicamente protegido, pues las evidencias no buscan directamente la protección de ese bien, sino que pretenden aportar datos que permitan acreditar los elementos objetivos y subjetivos del tipo penal"[11].

[8] Viega, María José. Pg. 178

[9] Navarro Isla, Jorge. Pg. 398-399

[10] Ibid. Pg. 399

[11] Ibid. Pg. 399

Los delitos informáticos no solo afectan a un bien jurídico determinado, sino que afectan a una diversidad de ellos poniendo en relieve los intereses colectivos, en tal sentido María Luz Gutiérrez Francés citada por Acurio del Pino, respecto de la figura del fraude informático nos dice que: "Las conductas de fraude informático presentan indudablemente un carácter pluriofensivo"[12]. En cada una de sus modalidades se produce una doble afección: la de un interés económico ya sea micro, como la hacienda pública, el sistema crediticio, el patrimonio, etc., y la de un interés macrosocial vinculado al funcionamiento de los sistemas informáticos.

El surgimiento de nuevas tecnologías provoca la existencia de nuevos elementos que atentan contra bienes tradicionales jurídicamente protegidos como la privacidad, el patrimonio, la intimidad, la seguridad nacional, etc., sin embargo también surgen nuevos bienes que se considera deberían ser protegidos jurídicamente, entre estos podemos mencionar la calidad, pureza e idoneidad de la información en cuanto tal, la confianza en los sistemas informáticos.

2.4. ELEMENTOS DE LOS DELITOS INFORMÁTICOS

Según el autor "Elías P. Gustavino" existen dos elementos esenciales para la comisión de los delitos informáticos que son los siguientes:

2.4.1. "Elemento Objetivo

Todo atentado que signifique dañar o desviar el correcto desempeño de la máquina con la finalidad de causar un perjuicio que redunde en beneficio material o moral para sí o para otro, constituye el elemento objetivo caracterizante del delito informático en su manifestación más común. En

[12] Del Pino, Acurio. Pg. 21

algunos casos la acción tiende a afectar elementos componentes de la computadora, tanto el hardware como el software, mientras que en otros la computadora sólo es utilizada como medio o instrumento para cometer el delito. También es posible que, sin afectar los componentes de una computadora ni utilizarla para la perpetración de un hecho ilícito autónomo, lo ilícito de la conducta consiste en el uso indebido de una computadora sin la correspondiente autorización.

2.4.2. Elemento Subjetivo

El elemento subjetivo debe estar constituido por el dolo o la culpa con que actúa el sujeto activo del delito informático"[13].

2.5. SUJETOS DE LOS DELITOS INFORMÁTICOS

Dentro del Derecho Penal, para la comisión de un determinado delito es necesaria la participación tanto del sujeto activo como del sujeto pasivo. De esta manera podemos decir que el titular del bien jurídico lesionado es el sujeto pasivo y, aquel que realiza la figura delictiva será denominado sujeto activo.
"Elías Gustavino" describe a los sujetos de los delitos informáticos de la siguiente manera:

2.5.1. Sujeto Activo

"Se caracterizan por ser personas de un determinado nivel de inteligencia y educación, superior al común. Estos pueden ser operadores cuando modifican, agregan, eliminan o sustituyen información o programas, o copian archivos para venderlos a competidores; programadores que violan o inutilizan controles

[13] Gustavino Elías. Pgs. 82-83

protectores del programa o sistema, informan a terceros ajenos a la empresa, atacan el sistema operativo, sabotean programas, modifican archivos o acceden a información confidencial; analistas de sistemas que generalmente son los únicos que conocen la operación completa de ellos; analistas de comunicaciones diseñadores de la seguridad del sistema de comunicaciones, por lo que conocen los métodos para violar dicha seguridad con fines de fraude; supervisores con conocimiento integral de las operaciones y debilidades del sistema de seguridad, pudiendo manipular archivos de datos y los ingresos y salidas del sistema; personal técnico y de mantenimiento, que suele tener libre acceso a los centros de cómputo y conocen los sistemas operativos y bases de datos.

2.5.2. Sujeto Pasivo

Entre los sujetos pasivos figuran las entidades financieras como víctimas frecuentes por la creciente utilización de transferencias de fondos de forma electrónica, donde se movilizan cantidades importantes de dinero mediante símbolos electrónicos como único tipo de registro"[14].

También podemos mencionar a las personas individuales como víctimas o sujetos pasivos de los delitos informáticos.

"El sujeto pasivo, tiene la particularidad que en la gran mayoría de los casos estos no son denunciados porque el descubrimiento del modus operando es difícil o por miedo al desprestigio de seguridad de sus sistemas y la consecuente pérdida económica que esto puede ocacionarles, haciendo que este tipo de delitos se mantenga dentro de las llamadas cifras negras". [15]

[14] Gustavino, Elías. Pgs. 83-84

[15] Arce Jofré, Jofré. Pg. 149

2.6. CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS

Los delitos informáticos han sido objeto de variadísimas clasificaciones, y se han tenido en cuenta a estos efectos: el perjuicio causado, el papel que el computador desempeñe en la realización del mismo, el modo de actuar, el tipo penal en que se encuadren, clase de actividad que implique según los datos involucrados.

2.6.1. Clasificación según Julio Téllez Valdés

Julio Téllez Valdés clasifica a los delitos informáticos en base a dos criterios:

"1. Como Instrumento o Medio

Podemos hablar de aquellas conductas que se vales de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

a) Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.).

b) Variación de los activos y pasivos en la situación contable de las empresas.

c) Planeación o simulación de delitos convencionales (robo, homicidio, fraude, etc.)

d) Robo de tiempo de computadora.

e) Lectura, sustracción o copiado de información confidencial.

f) Modificación de datos tanto en la entrada como en la salida.

g) Aprovechamiento indebido o violación de un código para penetrar a un sistema con el fin de introducir instrucciones inapropiadas (esto es lo que se conoce en el medio como método del Caballo de Troya).

h) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa, método conocido como la técnica de salami.

i) Uso no autorizado de programas de cómputo.

j) Insertar instrucciones que provocan interrupciones en la lógica interna de los programas, a fin de obtener beneficios.

k) Alteración en el funcionamiento de los sistemas.

l) Obtención de información residual impresa en papel o cinta magnética luego de la ejecución de trabajos.

m) Acceso de áreas informatizadas en forma no autorizada.

n) Intervención de las líneas de comunicación de datos o teleproceso."[16]

2. "Como Fin u Objeto

En esta categoría encuadramos a las conductas que van dirigidas en contra de la computadora, accesorios o programas como entidad física, como por ejemplo:

a) Programación de instrucciones que producen un bloqueo total al sistema.

b) Destrucción de programas por cualquier método.

c) Daño a la memoria.

d) Atentado físico contra la máquina o sus accesorios (discos, cintas, terminales, etc.).

e) Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.

f) Secuestro de soportes magnéticos en los que figura información valiosa con fines de chantaje, pago de rescate, etc."[17]

[16] Tellez Valdes,Julio. Pgs. 165-166

2.6.2. Clasificación según Jorge Pacheco Klein

Jorge Pacheco Klein, citado por María José Viega, clasifica a los delitos informáticos en:

a) "Delitos informáticos internos. Ej.: sabotaje de programas.
b) Delitos a través de las telecomunicaciones. Ej.: Hacking.
c) Manipulación de computadoras. Ej.: apropiación indebida, peculado y fraudes informáticos. Es la más vinculada a delitos de cuello blanco.
d) Utilización de computadoras en apoyo a empresas criminales, como el lavado de dinero y la distribución ilícita de drogas.
e) Robos de software (piratería)"[18]

2.6.3. Clasificación según Uhlrich Sieber

Uhlrich Sieber, citado por Carlos Correa, clasifica a los delitos informáticos en las siguientes categorías:

a) "Fraude por manipulaciones de un computador contra un sistema de procesamiento de datos;
b) Espionaje informático y robo de software;
c) Sabotaje informático;
d) Robo de servicios;
e) Acceso no autorizado a sistemas de procesamiento de datos; y
f) Ofensas tradicionales en los negocios asistidos por computador."[19]

---

[17] Tellez Valdes. Julio. Pg. 166

[18] Viega, María José. Pg. 180

2.6.4. Tipos de ataques contra los sistemas de información

En el texto Seguridad de las Redes y de la Información propuesta para un enfoque político europeo, citado por Julio Tellez Valdes, la Comisión de las Comunidades Europeas, propuso la descripción siguiente sobre las amenazas contra los sistemas informáticos:

a) "Acceso no autorizado a sistemas de información: esto incluye el concepto de piratería informática, la cual consiste en tener acceso de manera no autorizada a una computadora o a una red de computadoras, Puede tomar distintas formas que van desde el uso de informaciones internas a ataques directos y la interceptación de contraseñas. Se realiza generalmente pero no siempre con una intención dolosa de copiar, modificar o destruir datos. La corrupción deliberada de sitios Internet o el acceso sin previo pago a servicios restringidos puede constituir uno de los objetivos del acceso no autorizado.

b) La perturbación de los sistemas de información: existen distintas maneras de perturbar los sistemas de información mediante ataques malintencionados. Uno de los medios más conocidos de denegar o de deteriorar los servicios ofrecidos por Internet es el ataque de tipo **denegación de servicio (DdS).** Este ataque es en cierta medida similar al hecho de inundar las máquinas de fax con mensajes largos y repetidos. Los ataques del tipo denegación de servicio tienen por objeto sobrecargar los servidores o los proveedores de servicios Internet (PSI) con mensajes generados automáticamente. Otros tipos de ataques pueden consistir en perturbar los servidores que hacen

[19] Correa Carlos. Pg. 296

funcionar el sistema de nombres dominio (DNS) y los ataques contra los encaminadotes. Los ataques destinados a perturbar los sistemas han sido perjudiciales para algunos sitios web prestigiosos como los portales. Según estudios, ataques de estos causan daños estimados en varios centenares de millones de dólares, sin contar el perjuicio no cuantificable en términos de reputación. Las empresas cuentan cada vez más con un sitio web propio y las que dependen de él para el suministro justo a tiempo son especialmente vulnerables.

c) Ejecución de programas informáticos perjudiciales que modifican o destruyen datos: el tipo más conocido de programa informático malintencionado es el virus. Los virus "I love you", "Melisa" y "Kournikova" son ejemplos. Existen otros tipos de programas informáticos perjudiciales. Algunos dañan a la proia computadora, mientras que otros utilizan el PC para atacar otros elementos de la red. Algunos programas (llamados "bombas lógicas") pueden permanecer inactivos hasta que se desencadenan por algún motivo, como por ejemplo, una fecha determinada, causando graves daños modificando o destruyendo datos. Otros programas parecen benignos, pero cuando se activan, desencadenan un ataque perjudicial (por eso se llama Caballos de Troya). Otros programas llamados gusanos no infectan programas con virus, pero crean réplicas de ellos mismos, éstas crean a su vez nuevas réplicas y de este modo se termina por invadir el sistema.

d) Intervención de las comunicaciones: La intervención malintencionada de comunicaciones afecta los requisitos de confidencialidad e integridad de los usuarios. Se le denomina a menudo Sniffing (intromisión).

e) Declaraciones falsas: los sistemas de información ofrecen nuevas posibilidades de declaraciones falsas y de fraude. El hecho de usurpar la identidad de otra persona en Internet y de utilizarla con

fines malintencionados se llama spoofing (modificación de los datos)"[20].

2.7. SEGURIDAD Y/O PREVENCIÓN INFORMÁTICA

Debido al incremento de los delitos informáticos a nivel mundial y a la aparición de nuevas figuras delictivas relacionadas con los cambios que sufre la tecnología día a día tenemos la necesidad imperiosa de tratar de encontrar formas de control adecuadas a esta realidad para de esta manera poder prevenir este tipo de comportamientos ilícitos.

Según Julio Tellez Valdes existen dos formas de control, las cuales se describen a continuación:

2.7.1. Formas de Control

- **"Preventivo**

Este tipo de ilícitos requiere de un necesario control, y este, al no encontrar en la actualidad un adecuado entorno jurídico, ha tenido que manifestarse, en su función preventiva, a través de diversas formas de carácter administrativo, normativo y técnico, de entre las que se cuentan las siguientes:

a) Elaboración de un examen psicométrico previo ingreso al área de sistemas en las empresas.
b) Introducción de cláusulas especiales en los contratos de trabajo, con el personal informático, que por el tipo de labores a realizar así lo requiriera.
c) Establecimiento de un código ético de carácter interno en las empresas.

[20] Tellez Valdes, Julio. Pgs. 166-167

d) Adoptar estrictas medidas en el acceso y control de las áreas informáticas de trabajo.

e) Capacitación adecuada del personal informático, a efecto de evitar actitudes negligentes.

f) Identificación, y en su caso segregación del personal informático descontento.

g) Rotación en el uso de claves de acceso al sistema (passwords).

h) Auditoría Informática."[21]

- **"Correctivo**

Esto podrá darse en la medida en que se introduzca un conjunto de disposiciones jurídicas específicas en los códigos penales sustantivos, ya que en caso de considerar este tipo de ilícitos como figuras análogas "existentes", se corre el riesgo de alterar flagrantemente el principio de legalidad de las penas. (Nulla pena sine legem).

Cabe hacer mención que una adecuada legislación al respecto traería consigo efectos no sólo correctivos sino eventualmente preventivos, de forma que se reducirían en buen número este tipo de acciones que tanto daño causan a los intereses individuales y sociales, inhibiendo la eventual comisión de estos delitos.

El objetivo de la creación de un espacio de libertad, seguridad y justicia debe ser alcanzado mediante la prevención y la lucha contra la delincuencia organizada o no, incluido el terrorismo, mediante una cooperación más estrecha entre los servicios represivos y las autoridades judiciales de los distintos Estados interesados, al uniformar las legislaciones y las normas en

[21] Tellez Valdes, Julio, Pg. 175

materia de cooperación policial y judicial penal, la reciente entrada en funciones de la Corte Penal Internacional (Estatuto de Roma) pone de relieve la necesidad de pensar cada vez más, en una "universalización" del Derecho."[22]

[22] Tellez Valdes, Julio. Pg. 176

CAPITULO III
ESTAFA ELECTRÓNICA

3.1. CONCEPTO

El concepto de "Estafa Electrónica" es conocido en el ámbito internacional en sus diferentes denominaciones como "Fraude Informático", "Estafa Informática", "Estafa Computacional", "Fraude Cibernético" entre otros. Esto debido a que este tipo de delito es considerado como nuevo, mismo que debe ser regulado en el ámbito penal para una correcta sanción.

"El fraude informático, también conocido bajo la figura de Estafa Electrónica en varias legislaciones, consiste en la transmisión no consentida de activos a través de la manipulación o alteración de datos informáticos. Entonces, se trata de una conducta paralela a la de la estafa en la que la conducta del sujeto activo, guiada por el ánimo de lucro, se dirige a la provocación de una disposición patrimonial, pero en la que el mecanismo defraudatorio no es propiamente una provocación, mediante engaño, de un error en la víctima, sino la manipulación de un sistema informático"[1].

"Esta modalidad delictiva también conocida como "Fraud by Computer Manipulation", se puede desarrollar a través de manipulaciones a los usuarios de Internet, a los programas de funcionamiento de sistemas informáticos y telemáticos o a los contenidos de bases de datos, afectando de este modo el almacenamiento, procesamiento o transferencia de datos o información informatizada, el patrimonio económico o la administración pública, así por ejemplo el "financial institution fraud", que consiste en inducir a una persona en error con el propósito de realizar negocios de crédito o capital en la web, o de

[1] Rico Carrillo, Mariliana. Pg. 210

realizar una actividad de crédito mediante fraudes de banca electrónica; el "Gramming fraud", en el cual se solicita dinero o valores a un sujeto, creando una falsa expectativa de ganancias que luego se incumple (apuestas y casinos on line); el "advance fee fraud", los "pbony scrow services" y las compras y ventas fraudulentas (los fraudes de boletos de avión), en los cuales el sujeto pasivo es instado a pagar abonos en dinero significativos, para recibir servicios, más dinero o mercancías que no se envían o se incumplen; los fraudes a compañías de seguros, fraudes a la confianza que terminan en pérdidas financieras; el "spoofing/phisching" en los que el defraudador personifica una identidad ajena (en la web o vía e-mail) para obtener beneficios ilícitos u obtener información confidencial de los usuarios; las manipulaciones en el pago de sueldos, facturas, subsidios, etc."[2]

Los delitos informáticos en sentido estricto implican hipótesis especiales de apoderamiento o sustracción de datos o información con ánimo de lucro genérico (hurto de tiempo informático o de servicios que impliquen erogaciones importantes para la empresa o su titular) o de defraudación informática en las que no existe inducción o mantenimiento en error de una persona, sino más bien manipulación, introducción, alteración, borrado o supresión de datos, sistemas, redes, programas, bases de datos o de los resultados del procesamiento de datos con ánimo de lucro o de beneficio, que conllevan una defraudación potencial no consentida a los intereses económicos de las víctimas en provecho de los defraudadores o terceros. Situaciones que no quedan cubiertas por los tipos tradicionales. La diferencia entre ambas modalidades criminales es evidente: los tipos económicos tradicionales generalmente vinculan la acción de despatrimonialización a objetos de naturaleza material, mientras que los delitos informáticos en sentido estricto vinculan la conducta con objetos de naturaleza inmaterial con repercusiones indirectas en el ámbito patrimonial.

[2] Posada Maya, Ricardo. Pg. 42

"Se habla también de una modalidad delictiva conocida en el mundo informático como "salami" o Slicing" o "jaleteo", consiste en una forma de realización continuada del tipo penal, a través de la cual, el agente (insider o outsider) – haciendo uso de un software especial que introduce datos u órdenes falsas o efectúa alteraciones en los programas que gestionan automáticamente transferencias bancarias o reconocimientos de créditos a favor del agente- mantiene en error operativo a la entidad, y se apropia de pequeñas cantidades de dinero que son sustraídas automáticamente del redondeo de cifras mayores en la liquidación de cuentas o de sus respectivos intereses, esta modalidad también podaría ser cubierta por el tipo penal de estafa, en su modalidad de transferencia de activos patrimoniales no consentidos mediante artificios en perjuicio de terceros."[3]

3.2 CLASIFICACIÓN DE LA ESTAFA ELECTRÓNICA

Existen diferentes figuras delictivas contrarias a la ley que se encuadran dentro de lo que se denomina "Estafa Electrónica", mismas que son descritas por Acurio del Pino de la siguiente manera:

3.2.1. Datos Falsos o Engañosos (Data Diddling)

"Conocido también como introducción de datos falsos o manipulaciones de datos de entrada, es la manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Este tipo de fraude informático representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede

[3] Posada Maya, Ricardo. Pg. 44

realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos."[4]

3.2.2. Manipulación de Programas o "Caballo de Troya" (Troya Horses)

"Es muy difícil de descubrir y a menudo pasa inadvertido debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Un método común utilizado por las personas que tienen conocimientos especializados en programación informática, es el denominado Caballo de Troya que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal."[5]

3.2.3. Técnica del Salami (Salami Technique Rounching Down)

"Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra. Consiste en introducir al programa instrucciones para remitir a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes."[6]

[4] Del Pino Acurio, Pg. 23

[5] Ibid. Pg. 23

[6] Del Pino, Acurio. Pg. 23

3.2.4. Falsificaciones Informáticas

"Como objeto: Cuando se alteran datos de los documentos almacenados en forma computarizada.

Como instrumento: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial.

Cuando empezó a disponerse de fotocopiadoras computarizadas en color basándose en rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer reproducciones de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos"[7].

3.2.5. Manipulación de los Datos de Salida

"Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían basándose en tarjetas bancarias robadas, sin embargo, en la actualidad se usa ampliamente equipo y programas de computación especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito"[8].

[7] Ibid. Pg. 23

[8] Del Pino, Acurio. Pg. 24

3.2.6. Pishing

"Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños.

Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. El robo de identidad es uno de los delitos que más ha aumentado. La mayoría de las víctimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es aún peor. En los últimos cinco años diez millones de personas han sido víctimas de delincuentes que han abierto cuentas de tarjetas de crédito o con empresas de servicio público, o que han solicitado hipotecas con el nombre de las víctimas, todo lo cual ha ocasionado una red fraudulenta que tardará años en poderse desencadenar.

Existe también una nueva modalidad de Pishing que es llamado Spear Pishing o Pishing segmentado, el cual ataca grupos determinados, es decir se busca grupos de personas vulnerables a diferencia de la modalidad anterior"[9].

3.3. ELEMENTOS DE LA ESTAFA ELECTRÓNICA

Inicialmente, Este tipo de delitos requería para su producción dos elementos claros:

[9] Ibid. Pg. 24

- La utilización de engaño bastante por el autor del delito.
- La producción de un error en la víctima del mismo.

La necesidad de concurrencia de estos dos elementos ha impedido en muchas ocasiones poder clarificar un hecho como estafa cuando ha tenido lugar mediante la utilización de un medio informático o cuando éste ha estado presente en la acción delictiva de cualquier otra forma. Por ejemplo, no es posible subsumir la estafa realizada por una persona utilizando el ordenador de su casa logrando la transferencia bancaria de la cuenta de un tercero a una de su titularidad.

En este supuesto sí existe el ánimo de lucro puesto que el estafador actúa guiado por ese afán de enriquecerse económicamente, y el perjuicio a tercero, puesto que se produce un detrimento económico a otra persona, pero sin embargo no aparecen estos dos elementos anteriormente señalados, el engaño a tercero y el error bastante, y ello porque el autor del delito no ha utilizado ninguna treta ni artimaña para engañar a la víctima, para viciar la voluntad del tercero, puesto que la acción se ha producido a través de una máquina, el ordenador, y como consecuencia tampoco cabe plantearse la producción de error por el mismo motivo.

Es por ello que en los casos en que se producían estas defraudaciones informáticas, la doctrina y la jurisprudencia se vieron obligadas a acomodarlas a las figuras ya existentes, sin embargo se comprobó que no era factible.

Entonces, los principales elementos que constituyen el delito de fraude o estafa informática son:

- El ánimo de lucro

- La acción típica es la de valerse de una manipulación informática o artificio semejante, desapareciendo de esta manera el engaño bastante y el error.
- La transferencia no consentida del patrimonio de otra persona sin utilizar violencia.
- Perjuicio a tercero.

El ánimo de lucro se refiere a que el sujeto activo actúe con el deseo o la intención de enriquecerse, de aumentar su patrimonio.

El concepto de manipulación informática corresponde con la conducta de alterar, modificar u ocultar datos informáticos de manera que se realicen operaciones de forma incorrecta o que no se lleven a cabo, y también con la conducta de modificar las instrucciones del programa con el fin de alterar el resultado que se espera obtener. De esta forma un sujeto puede introducir instrucciones incorrectas en un programa de contabilidad de manera que no anote cargos a su cuenta corriente por ejemplo, o que desplace a su cuenta bancaria todos los ingresos efectuados un determinado día a las cuentas cuyos números terminen en determinado número, etc.

La transferencia no consentida está referida al cambio de una partida económica de un lugar a otro, es decir, desplazamiento de dinero de la cuenta bancaria de la víctima a la cuenta del autor del delito.

El perjuicio debe afectar a un tercero, ya que no es la propia víctima la que realiza la transferencia económica, sino que es el propio autor del delito el que la lleva a cabo.

En este delito no cabe la comisión culposa, el sujeto activo actúa dolosamente, es decir, actúa conociendo y queriendo realizar la acción delictiva. El concepto de

"manipulación informática" implica por sí mismo, la intencionalidad del sujeto activo, es difícil que alguien lleve a cabo actos de alteración, modificación de datos o programas informáticos por error y que además le reportan un beneficio económico, ya que estas acciones requieren conocer los datos o instrucciones correctas y cambiarlos por otros, el sujeto sabe que su actuación constituye una acción contraria a derecho y aún así la lleva a cabo.

3.4. REQUISITOS DE LA ESTAFA ELECTRÓNICA

Según Miguel Ángel Moreno Navarrete son cuatro los requisitos esenciales para que un delito sea considerado como Estafa Electrónica:

a) "Que se produzca a través de medios informáticos.

b) Que no exista consentimiento.

c) Que se produzca la efectiva transferencia patrimonial.

d) Que sea en perjuicio de tercero."[10]

3.5. CARACTERÍSTICAS DE LA ESTAFA ELECTRÓNICA

A continuación se detallaran las características típicas de la estafa electrónica según Mariliana Rico Carrillo, para un mejor análisis:

3.5.1. Conductas delictivas en los instrumentos de pago

> "Entre los mecanismos de pago más utilizados en la actualidad, dentro y fuera de Internet, se encuentran las tarjetas en sus distintas modalidades y las transferencias electrónicas de fondos, aunque estos no son los únicos dispositivos que permiten realizar pagos en forma electrónica. El avance de las TIC, junto con el desarrollo de las operaciones comerciales en Internet, ha propiciado la creación de diversos mecanismos e

[10] Moreno Navarrete, Miguel Ängel. Pg. 154

instrumentos de pago, tal es el caso de los cheques y las letras de cambio electrónicas, el dinero efectivo electrónico almacenado en el disco duro de los computadores y los pagos a través de cuentas de correo electrónico"[11].

"El desarrollo de los instrumentos electrónicos de pago junto con el avance de la informática y la aparición de Internet han propiciado el surgimiento de nuevas conductas delictivas, a la vez que han contribuido a la creación de ciertos patrones en la comisión de algunos delitos que dificultan su encuadramiento en los tipos penales tradicionales; la mayoría de ellos se encuentran directamente relacionados con las tarjetas de pago. Algunas de estas conductas se encuadran dentro de los delitos informáticos, en tanto que otras son supuestos de criminalidad en Internet."[12]

"En el estudio de los supuestos delictivos cometidos a través de medios de pago es necesario diferenciar cuando el delito tiene por objeto el medio de pago en sí, como es el caso de la clonación de tarjetas, la falsificación, el tráfico y el apoderamiento indebido de datos, y cuando el medio de pago es el instrumento utilizado para la comisión de un delito que tiene lugar a través del uso ilícito del medio de pago –o de los datos asociados- y se materializa en la disposición indebida del dinero."[13]

A) Conductas que tienen como objeto el instrumento de pago

Este tipo de conductas conducen a la utilización ilícita del instrumento de pago, que normalmente se traduce en la disposición indebida del dinero o

[11] Rico Carrillo, Mariliana. Pg. 211

[12] Ibid. Pg. 211

[13] Rico Carrillo, Mariliana. Pg. 211

del crédito asociado (en el caso de las tarjetas de crédito), con el correspondiente perjuicio económico para el titular legítimo, quien es el único autorizado para la utilización del instrumento de pago. Estas conductas se encuadran, en la mayoría de los casos, en el "delito de estafa" y son los siguientes:

a) La clonación de tarjetas

"Término que se utiliza actualmente para designar el fenómeno de la reproducción fraudulenta de tarjetas de pago que se lleva a cabo a través de la duplicación de los datos, normalmente contenidos en la banda magnética del instrumento original."[14]

"Los casos más frecuentes de clonación ocurren en los comercios tradicionales y en los cajeros automáticos y se llevan a cabo mediante el uso de un dispositivo electrónico conocido como skimmer, que permite copiar los datos de la banda magnética de la tarjeta. Una vez que los datos han sido copiados, son procesados a través de un equipo informático y un software que capta la información y permite incorporarla a una tarjeta nueva, creando de esta manera la duplicación de la tarjeta original. La utilización de este dispositivo ha generado el uso del término Skimming como omnicomprensivo de las situaciones donde se produce el robo de la información de las tarjetas como consecuencia de una utilización legítima del instrumento de pago"[15].

"En el ámbito de la Unión Europea, en el Dictamen del Comité Económico y Social sobre "la lucha contra el fraude y la falsificación

[14] Ibid. Pg. 212

[15] Rico Carrillo, Mariliana. Pg. 212

de los medios de pago distintos del efectivo", de 2009, se menciona la necesidad de prevenir y sancionar como delito la clonación de soportes plásticos con códigos y las contraseñas de las tarjetas de pago"[16].

b) La Falsificación

"En el ámbito de las tarjetas, la falsificación puede darse como consecuencia de la clonación –de hecho es su natural resultado-; sin embargo, también puede darse el supuesto de elaboración de tarjetas falsificadas independientemente de un proceso de clonación, donde la conducta se limita a la fabricación de un nuevo instrumento de pago mediante la copia de los datos del instrumento original. En la mayoría de estos casos, la elaboración de instrumento de pago se produce como consecuencia de un ataque informático (Hacking) a las empresas propietarias de tarjetas que mantienen bases de datos con la información de esos medios de pago."[17]

"La falsificación de instrumentos electrónicos de pago, donde se incluyen los cheques electrónicos y el dinero efectivo electrónico, también tiene lugar cuando se produce una alteración de los datos originalmente incorporados en los documentos representativos de estos medios de pago."[18]

c) Captación y uso indebido de datos: Phishing y Pharming

"La captación de datos es una práctica que facilita la comisión de otro delito que se perpetra a través del uso de esos datos con fines

[16] Ibid. Pg. 212

[17] Ibid. Pg. 213

[18] Rico Carrillo, Mariliana. Pg 213

fraudulentos. En el caso de las tarjetas, es frecuente la utilización de la información del instrumento de pago en las operaciones a distancia, principalmente por teléfono e Internet, donde la falta de presencia física permite que la transacción se lleve a cabo únicamente con los datos asociados al instrumento de pago"[19].

También se puede hacer referencia al phishing y al pharming como prácticas sofisticadas para el apoderamiento y captación de datos. En el primer caso "la captación ilícita de datos tiene lugar a través del envío masivo de correos electrónicos que simulan la identidad de una institución financiera con el objetivo de solicitar a los receptores los datos de sus respectivas tarjetas, alegando diversos motivos (promoción de productos o servicios, participación en concursos, problemas de seguridad, técnicos, etc.). Los correos electrónicos incluyen enlaces a sitios Web que imitan los de las entidades bancarias donde el usuario suministra los datos del instrumento de pago"[20].

"La técnica utilizada en el pharming también remite a los usuarios a páginas Web falsas, creadas en formato similar a las de las entidades bancarias con el objeto de captar los datos de los clientes. En estos casos, el procedimiento no se lleva a cabo mediante el envío masivo de correos electrónicos; el acceso indebido se produce por una vulnerabilidad en el DNS (Domain Name System) o en el de los equipos de los usuarios, que permiten al ataque redirigir el nombre de

[19] Ibid. Pg. 213

[20] Rico Carrillo, Mariliana. Pg. 214

dominio de la entidad a una página Web que en apariencia es idéntica."[21]

La utilización de este tipo de información con fines fraudulentos denota la captación indebida de datos realizada mediante engaños y en beneficio propio

B) Conductas derivadas de la utilización del instrumento de pago: Los supuestos de estafa

"La realización de las conductas anteriormente descritas no tienen otra finalidad que lograr la disposición indebida del dinero o del crédito asociado a la tarjeta, con el perjuicio patrimonial que esto supone para el verdadero titular. Aunque en la mayoría de los caos la utilización de la tarjeta –o de los datos del instrumento de pago- por terceras personas configura el supuesto de estafa, en la práctica se han dado situaciones que dificultan su encuadramiento en tal figura, al menos en su concepción tradicional, al no estar presentes los tres elementos que caracterizan este supuesto delictivo: el engaño, seguido del error y de la disposición patrimonial."[22]

En lo que se refiere a la estafa se observa que para que se de la comisión de este delito es necesaria la presencia física de la persona, y que mediante esta acción delictiva se tenga un beneficio indebido mediante engaños e induciendo a la víctima a error.

3.6. BIEN JURÍDICO PROTEGIDO

En el caso de los delitos informáticos referentes a estafa electrónica el bien jurídico

[21] Ibid. Pg. 214

[22] Rico Carrillo, Mariliana. Pg. 214-215

protegido es esencialmente el patrimonio de las personas afectadas por la comisión de estos delitos.

Según Miguel Ángel Moreno Navarrete también se protege "el comercio electrónico"[23]

3.7. MEDIAS DE SEGURIDAD PARA EVITAR EL DELITO DE ESTAFA ELECTRÓNICA

Es necesario establecer medidas de seguridad informática oportunas para evitar la proliferación de estos delitos y la suplantación de personalidad en las transacciones electrónicas que se lleven a cabo de forma automática a través de la Web.

Se debe exigir que los pagos se efectúen a través de sistemas establecidos previamente por entidades bancarias que dispongan de banca electrónica o galerías comercial electrónica, con el fin de garantizar que conocen a los clientes que efectúan la compra.

En la medida de los posible, utilizar entidades certificadoras que garanticen la identidad de la parte compradora y, exija el uso de sistemas de firma digital apropiados en los contratos con usuarios que deseen formalizar una relación continuada.

Establecer un límite cuantitativo a partir del cual todas las transacciones precisarán una autorización personal del responsable de crédito de la empresa de manera que el riesgo de estafa electrónica se limite a transacciones de pequeña cuantía.

[23] Moreno Navarrete, Miguel Ángel. Pg. 150

Exigir sistemas garantizados de pago en efectivo, tipo monedero electrónico, de manera que las pequeñas transacciones queden garantizadas.

Contratar un seguro que cubra las posibles pérdidas ocasionadas por estafas electrónicas sufridas en el desarrollo de su actividad de comercio electrónico.

CAPITULO IV
LEGISLACIÓN BOLIVIANA

Debido a la enorme importancia del tema de investigación y a la urgente necesidad de tener una correcta normativa con respecto a los delitos informáticos relacionados con la "Estafa Electrónica" por considerarse uno de los delitos más comunes en nuestro entorno y, para poder de esta manera frenar este tipo de actos delictivos y poder sancionarlos de manera adecuada, a continuación se realizará un análisis de lo que nuestro ordenamiento jurídico penal regula sobre el tema en cuestión.

4.1. CÓDIGO PENAL BOLIVIANO

El Código Penal Boliviano mediante Ley No. 1768 de 11 de marzo de 1997 "Ley de Modificaciones del Código Penal" tipifica los delitos informáticos de la siguiente manera:

Artículo 363 bis (MANIPULACIÓN INFORMÁTICA)

"El que con la intención de obtener un beneficio indebido para si o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno (1) a cinco (5) años y con multa de sesenta (60) a doscientos (200) días"[1].

(C.P.335, 345, 362, 363 ter)

[1] Código Penal Boliviano

Según el autor boliviano Arce "este tipo penal prevé aquella conducta por la cual se modifica información ya sea en el momento de su procesamiento o de su transmisión, es decir en el momento en que esa información esta siendo procesada por un sistema informático o cuando después de haber sido procesada, es transmitida. Para que esta conducta constituya delito debe producirse una transferencia patrimonial en perjuicio de un tercero y generar un beneficio indebido."[2]

Artículo 363 ter (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS)

El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año (1) o multa hasta doscientos (200) días.

(C.P. 335, 346, 363 bis)

"En el caso del Artículo 363 ter, se observa que el tipo penal exige que la acción realizadora del tipo (el acceso no autorizado a un sistema informático, para apoderarse, utilizar, modificar o inutilizar información) debe derivar en un resultado típico (ocasionar perjuicio a un tercero).

- En este tipo penal se está protegiendo, la integridad del sistema mismo y de la información procesada o contenida en él, los denominados "virus informáticos" son precisamente un ejemplo de destrucción o supresión de la información."[3]

[2] ArceJofré, Jofré. Pg. 150

[3] Ibid. Pg.151

Dentro de la legislación boliviana, hablando del Código Penal Boliviano, el artículo 335 hace referencia al delito de Estafa, y dice a la letra:

Artículo 335. (Estafa)

El que con la intención de obtener para sí o un tercero un beneficio económico indebido, mediante engaños o artificios provoque o fortalezca error en otro que motive la realización de un acto de disposición patrimonial en perjuicio del sujeto en error o de un tercero, será sancionado con reclusión de uno (1) a (5) años y con multa de sesenta (60) a doscientos (200) días.

(C.P. 204, 236, 234 bis-C.P.M. 226-C. Com. 1673)

Del análisis de las normas legales detalladas anteriormente, referidas a la Manipulación informática, se llega a la conclusión, de que si bien nuestro ordenamiento jurídico penal sanciona como delito cuando una persona con intención de obtener un beneficio indebido para si o un tercero, manipule un procesamiento o transferencia de datos informáticos, no es menos cierto que las normas en estudio se encuentran algo retrasadas debido al constante avance de la electrónica, es por esta razón que no existe una tipificación apropiada, amplia y precisa en lo que se refiere a los llamados nuevos delitos informáticos como es la "Estafa Electrónica", llegando a la conclusión de que la legalización boliviana en lo que se refiere a los delitos informáticos no es suficiente y merece ser reordenada y ampliada.

4.2. INCIDENCIA DENTRO DE NUESTRA SOCIEDAD

La proliferación de los delitos informáticos ha hecho que nuestra sociedad sea cada vez más escéptica a la utilización de tecnologías de la información, las cuales pueden ser de mucho beneficio para la sociedad en general.

También se observa el grado de especialización técnica que adquieren los delincuentes para cometer este tipo de delitos, por lo que personas con conductas maliciosas cada vez más están ideando planes y proyectos para la realización de actos delictivos, tanto a nivel empresarial como a nivel global.

Aquellas personas que no poseen los conocimientos informáticos básicos, son más vulnerables a ser víctimas de un delito, que aquellos que si los poseen. Aquel porcentaje de personas que no conocen nada de informática pueden ser engañadas si en un momento dado poseen acceso a recursos tecnológicos y no han sido asesoradas adecuadamente para la utilización de tecnologías como el Internet, correo electrónico, etc.

4.3. VACIOS LEGALES

En Bolivia, el año 1989, se consideró el análisis y tratamiento sobre Legislación Informática concerniente a contratación de bienes y servicios informáticos, flujo de información computarizada, modernización del aparato productivo nacional mediante la investigación científico-tecnológica en el país y la incorporación de nuevos delitos emergentes del uso y abuso de la Informática.

Este conjunto de acciones tendientes a desarrollar de manera integral la informática, se tradujo en el trabajo de especialistas y sectores involucrados, representantes en el campo industrial, profesionales abogados y especialistas informáticos, iniciándose la elaboración del Proyecto de Ley Nacional de Informática, concluido en febrero de 1991. Asimismo, el Código Penal Boliviano, texto ordenado según Ley No. 1768 de 1997, incorpora en el título X un capítulo destinado a los Delitos Informáticos. Ambos cuerpos legales tratan de manera general los nuevos delitos emergentes del uso de la Informática.

La Ley No. 1768, no obstante de no estar exenta de la problemática actual, al abordad el en Capítulo XI la tipificación y penalización de delitos informáticos, no contempla la descripción de estas conductas delictivas detalladas anteriormente, lo cual debilita la lucha contra estos ilícitos denominados "Delitos Informáticos". Por consiguiente, la atipicidad de las mismas en nuestro ordenamiento jurídico penal vigente imposibilita una clasificación jurídico-legal que individualice a las mismas, llegando a existir una alta cifra de criminalidad e impunidad, haciéndose imposible sancionar como delitos, hechos no descritos en la legislación penal con motivo de una extensión extralegal del ilícito penal ya que se estaría violando el principio de legalidad expreso en la máxima "Nullum crime sine lege".

CAPITULO V
LEGISLACIÓN COMPARADA

Con el objeto de contar con mayores elementos que nos permitan realizar un análisis más profundo, buscando siempre la posibilidad de sancionar como delito la "Estafa Electrónica", a continuación se realizará un análisis de las legislaciones de algunos países, normas que nos permitirán comentar y analizar la legislación boliviana.

5.1. COLOMBIA

> "La Ley 1273 por medio de la cual se modifica el Código Penal Colombiano, incluyen dentro de los bienes jurídicos tutelados a la información y los datos que se preservan integralmente en los sistemas que utilicen las tecnologías de la información y las comunicaciones. La Ley adiciona el Título "De la protección de la información y de los datos" y tipifica diversos delitos como el acceso abusivo a un sistema informático, la obstaculización ilegítima del mismo o de una red de telecomunicación la interceptación de datos informáticos, el daño informático, el uso de software malicioso, la violación de datos personales y la suplantación de sitios Web para capturar datos personales, considerando esta conducta como un atentado contra la confidencialidad, la integridad y la disponibilidad de los datos y los sistemas informáticos. Adicionalmente, sanciona el hurto por medios informáticos y la transferencia no consentida de activos realizada a través de estos medios"[1].
>
> El Código Penal colombiano, en su artículo 269J (modificado mediante Ley 1273) dice a la letra:

[1] Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. Pg. 11

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 1500 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."[2]

5.2. ESPAÑA

"En la jurisprudencia española anterior a la Reforma del Código Penal se observan diversos casos donde el juzgador advierte la imposibilidad de catalogar el supuesto de estafa, las compras con tarjetas ajenas por no existir el engaño suficiente en la víctima del hecho punible para producir el error. En algunos supuestos, la jurisprudencia determinó que la falta de diligencia de los aceptantes en el incumplimiento de sus deberes de comprobación de la identidad del titular impidió que se configurará el delito de estafa, al no estar presente uno de los elementos esenciales: el engaño."[3]

[2] www.oas.org/dil/esp/Código_penal_colombia.pdf

[3] Rico Carrillo, Mariliana. Pg. 215

"Otro problema que suscitó la definición tradicional de estafa en los supuestos de usos fraudulentos de tarjetas fue la imposibilidad de encuadrar en este tipo penal los usos ilícitos a través de cajeros automáticos, las manipulaciones en los terminales de puntos de venta (TPV) y las operaciones en Internet."[4]

"El desarrollo de las operaciones delictivas a través de medios informáticos condujo a una primera modificación del Código Penal en este ámbito. En la Reforma de 1995 se introdujo el delito de "Estafa Informática", donde se sustituye el término "engaño" por el de "manipulación informática". Aunque la construcción de este tipo penal constituyó un avance en la materia, ya que permitió sancionar diversos delitos relacionados con las tarjetas (captación de datos, falsificación, manipulación de cajeros automáticos y TPV, entre otros) los supuestos que se contemplaron en la norma también originaron problemas de interpretación que impidieron encuadrar en la estafa informático la utilización de tarjetas por terceros no autorizados en Internet."[5]

a) La Reforma de 2010

"El Código Penal Español fue reformado en 2010, gracias a la aprobación de la Ley Orgánica 5/2010 de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal."[6]

"Esta modificación obedece a la necesidad de adaptar las normas penales españolas a las exigencias de armonización jurídica exigidas por la Unión Europea. La reforma sigue las directrices de la Decisión Europea de 2001 al introducir los nuevos supuestos delictivos relacionados con los fraudes

[4] Rico Carrillo, Mariliana, Pg. 215

[5] Ibid. Pg. 215

[6] Ibid. Pg. 217

cometidos a través de instrumentos de pago, en particular la estafa y la falsificación de tarjetas."[7]

b) Los nuevos supuestos delictivos

a) La estafa a través de instrumentos de pago

"En su redacción actual, el delito de estafa, previsto en el artículo 248 del Código Penal, incluye la estafa clásica, genérica o convencional –como la denomina la doctrina-, la estafa informática y la estafa cometida a través de tarjetas de crédito, débito y cheques de viajero. Esta última categoría de estafa, que podemos denominar estafa a través de instrumentos de pago, es incorporada en el tipo delictual tras la reforma de 2010, ante los problemas interpretativos que se presentaron para catalogar la utilización de tarjetas ajenas en Internet en los tipos penales de estafa clásica y estafa informática."[8]

"En la concepción tradicional del delito de estafa sólo eran susceptibles de engaño las personas físicas, situación que acarreó una serie de problemas en la práctica a la hora de encuadrar en la estafa clásica los supuestos de estafa producidos a través de máquinas. Para solventar este tipo de situaciones, en la reforma del Código Penal de 1995 se agregó el tipo penal de la estafa informática, donde se sustituye el término engaño por el de manipulación informática, entendiéndose por tal la actuación de los sujetos sobre un sistema informático, de manera que tal actuación

[7] Rico Carrillo, Mariliana, Pg. 217

[8] Ibid. Pg. 217

altere el resultado que habría de conducir el normal procesamiento automatizado de datos."[9]

"Se consideran reos de estafa: "Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero"[10].

"La inclusión de este tipo penal abarca las operaciones de pago presenciales y las operaciones de pago que se llevan a cabo a través de sistemas de comunicación a distancia, toda vez que la norma no hace distinción sobre el lugar donde el instrumento de pago es utilizado, y se refiere en general a operaciones de cualquier clase en perjuicio del titular o de un tercero."[11]

"Aunque en la mayoría de los pagos presenciales con tarjetas ajenas se configura el delito de estafa clásica, en la práctica se han presentado casos que han originado serias dificultades para encuadrar estas conductas en el tipo penal de estafa, al no mediar engaño suficiente para producir error en la víctima. En atención a la nueva redacción del artículo 248 del Código Penal, todos los supuestos de utilización fraudulenta de una tarjeta ajena serán objeto de sanción penal, con independencia de la actuación del aceptante, que entra en el calificativo de "tercero" empleado en la redacción de la norma."[12]

[9] Rico Carrillo Mariliana . Pg. 217

[10] Ibid. Pg. 218

[11] Ibid. Pg. 218

[12] Rico Carrillo, Mariliana, Pg. 218

b) Falsificación de Instrumentos de Pago

"En la reforma de 2010, el delito de falsificación de moneda se delimita única y exclusivamente a la moneda metálica y al papel moneda decurso legal, tal como se observa en la redacción del actual artículo 386 del Código Penal, esto obedece a la necesidad de crear un nuevo tipo penal autónomo e independiente, destinado a sancionar el fraude cometido a través de la falsificación de instrumentos de pago, circunstancia que se expresa en el propio texto de la exposición de motivos de la Ley 5/2010, donde se indica que:

Las tarjetas de crédito o débito requieren también su propia tutela frente a la falsificación, a cuyo fin se describe específicamente esa conducta referida a ellas o a los cheques de viaje. La comprobada frecuencia con la que estas actividades delictivas se descubren como propias de organizaciones criminales obliga al establecimiento de las correspondientes previsiones represoras. La tutela penal se extiende a su vez al tráfico con esos instrumentos falsos y a su uso y tenencia en condiciones que permitan inferir su destino al tráfico, aunque no se haya intervenido en la falsificación."[13]

"Actualmente, el delito de falsificación de instrumento de pago se encuentra tipificado en el artículo 399 bis, relativo a la falsificación de tarjetas de crédito y débito y cheques de viaje, incluido en la sección 4 del capítulo II del Código Penal, que penaliza las falsificaciones documentales. El precepto castiga a quienes alteren, copien, reproduzcan, o de cualquier otro modo falsifiquen tarjetas de crédito o débito o cheques

[13] Ibid. Pg. 219

de viaje, la tenencia y el uso de estos instrumentos a sabiendas de la falsedad también es objeto de sanción penal."[14]

c) **Phishing y Pharming**

"Desde la óptica del derecho penal español, las conductas constitutivas de phishing y pharming se encuadran en el delito previsto en el artículo 248.2 del Código Penal, donde se tipifica la estafa informática. En lo que se refiere al phishing, si bien la mayoría de la jurisprudencia lo ha calificado como tal, un sector de la doctrina estima que en estos casos se trata de una estafa clásica, que se produce al engañar al titular de la cuenta defraudada mediante el envío del mensaje."[15]

"Tanto en le phishing como en le pharming existe una manipulación informática que se lleva a cabo a través de las acciones encaminadas a duplicar la página Web de la entidad financiera, con la finalidad de captar los datos de instrumento de pago y obtener una transferencia patrimonial no consentida en perjuicio de un tercero, supuesto contemplado en el artículo 248.1 del Código Penal Español."[16]

"A pesar de su caracterización como estafa, la tipificación de estos delitos no se agota en esta modalidad, ya que se trata de todo un complejo delictivo que exige la realización de diversos pasos hasta llegar a la transferencia no consentida del dinero. En ambos casos el modus operando exige la elaboración de una página Web falsa, cuya acción en el

[14] Rico Carrillo, Mariliana. Pg. 219

[15] Ibid. Pg. 220

[16] Ibid. Pg 220

marco del Código Penal Español se encuadra en el delito de falsedad documental, tipificado en el artículo 392."[17]

5.3. VENEZUELA

"En materia penal, destaca la Ley Especial Contra Delitos Informáticos, que tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías. Dentro de los delitos tipificados se encuentra el acceso indebido a los sistemas informáticos, el sabotaje o daño a los mismos, el espionaje informático y la falsificación de documentos electrónicos. También sanciona diversos delitos contra la propiedad, particularmente los referidos a la obtención de información perteneciente a terceros para apropiarse de sus bienes o valores, así como el fraude cometido a través del uso de tecnologías de información, el manejo fraudulento de tarjetas inteligentes, la provisión indebida de bienes o servicios y la posesión de equipo para falsificaciones."[18]

Al hablar de fraude informático esta Ley dice a la letra:

Artículo 14. Fraude. "Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de cualquier manipulación en sistemas o cualquiera de sus componentes, o en la data o información en ellos cometida, 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."[19]

[17] Rico Carrillo, Mariliana. Pg 220

[18] Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. Pg. 28

[19] www.oas.org/dil/esp/codigopenal_venezuela.pdf

5.4. ARGENTINA

"En el ámbito penal, la Ley 26.388 modificatoria del Código Penal, tipifica algunos delitos informáticos, tales como la interceptación de comunicaciones, el acceso ilícito a los sistemas de cómputo, el daño informático, el fraude, la falsificación de documentos electrónicos o informáticos, la interrupción de comunicaciones o alteración de pruebas digitales. De igual forma, mediante otras disposiciones como la Ley 25.036, castiga la violación de los derechos de propiedad intelectual vinculados con el software. De igual forma, mediante la Ley 25.506 castiga el delito de falsificación de firma digital y en virtud de la Ley de Inteligencia Nacional, tipifica el delito de violación de secretos e interceptación indebida de comunicaciones."[20]

En cuanto a estafa electrónica el Código Penal Argentino dice lo siguiente:

Capítulo IV. Estafas y otras defraudaciones

Artículo 172.- "Será reprimido con prisión de un mes a seis años, el que defraudare a otro con nombre o supuesto, calidad simulada, falsos títulos, influencia mentida, abuso de confianza o aparentando bienes, crédito, comisión, empresa o negociación o valiéndose de cualquier otro ardid o engaño."[21]

Artículo 173.- "Sin perjuicio de la disposición general del artículo prece4dente, se consideran casos especiales de defraudaciones y sufrirán la pena que él establece:

[20] Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. Pg. 4

[21] www.oas.or/dil/espcodigo penal de la republica argentina.pdf

1. El que defraudare a otro en la substancia, calidad o cantidad de las cosas que le entregue en virtud de contrato o de un título obligatorio;
2. El que con perjuicio de otro se negare a restituir o no restituyere a su debido tiempo, dinero, efectos o cualquier otra cosa mueble que se le haya dado en depósito, comisión, administración u otro título que produzca obligación de entregar o devolver;
3. El que defraudare, haciendo suscribir con engaño algún documento;
4. El que cometiere alguna defraudación abusando de firma en blanco extendiendo con ella algún documento en perjuicio del mismo que la dio o tercero;
5. El dueño de una cosa mueble que la sustrajere de quien la tenga legítimamente en su poder, con perjuicio del mismo o de tercero;
6. El que otorgare en perjuicio de otro, un contrato simulado o falsos recibidos;
7. El que, por disposición de la ley, de la autoridad o por un acto jurídico, tuviera a su cargo el manejo, la administración o el cuidado de bienes o intereses pecuniarios ajenos, y con el fin de procurar para si o para un tercero un lucro indebido o para causar daño, violando sus deberes perjudicare los intereses confiados u obligare abusivamente al titular de éstos;
8. El que cometiere defraudación, substituyendo, ocultando o mutilando algún proceso, expediente, documento u otro papel importante;
9. El que vendiere o gravare como bienes libres, los que fueren litigiosos o estuvieren embargados o gravados; y el que vendiere, gravare o arrendare como propios, bienes ajenos;

10. El que defraudare con pretexto de supuesta remuneración a los jueces u otros empleados públicos;
11. El que tomare imposible, incierto o litigiosos el derecho sobre un bien o el cumplimiento, en los condiciones pactadas, de una obligación referente al mismo, sea mediante cualquier acto jurídico relativo al mismo bien, aunque no importe enajenación, sea removiéndolo, reteniéndolo, ocultándolo o dañándolo, siempre que el derecho o la obligación hubieran sido acordados a otro por un precio o como garantía;
12. El titular fiduciario, el administrador de fondos comunes de inversión o el dador de un contrato de leasing, que en beneficio propio o de un tercero dispusiere, gravara o perjudicare los bienes y de esta manera defraudare los derechos de los contratantes; (Inciso incorporado por art. 82 de la Ley No. 24.441 B.O. 16/1/1995)
13. El que encontrándose autorizado para ejecutar extrajudicialmente un inmueble lo ejecutara en perjuicio del deudor, a sabiendas de que el mismo no se encuentra en mora, o maliciosamente omitiera complementar los recaudos establecidos para la subasta mediante dicho procedimiento especial (Inciso incorporado por art. 82 de la Ley No. 24.441 B.O. 16/1/1995)
14. El tenedor de letras hipotecarias que en perjuicio de deudor o de terceros omitiera consignar en el título los pagos recibidos. (Inciso incorporado por art. 82 de la Ley No. 24.441 B.O. 16/1/1995)
15. El que defraudare mediante el uso de una tarjeta de compra, crédito o débito, cuando la misma hubiere sido falsificada, adulterada, hurtada, robada, perdida u obtenida del legítimo emisor mediante ardid o engaño, o mediante el uso no

autorizado de sus datos, aunque lo hiciere por medio de una operación automática. (Inciso incorporado por art. 1 de la Ley No. 25.930 B.O. 21/9/2004)

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 (Inciso incorporado por art. 9 de la Ley No. 26388 B.O. 25/6/2008)"[22]

Artículo 174.- "Sufrirá prisión de dos a seis años:

1. El que para procurarse a sí mismo o procurar a otro un provecho ilegal en perjuicio de un asegurador o de un dador de préstamo a la gruesa, incendiare o destruyere una cosa asegurada o una nave asegurada o cuya carga o flete estén asegurados o sobre la cual se haya efectuado un préstamo a la gruesa;

2. El que abusare de las necesidades, pasiones o inexperiencia de un menor o de un incapaz, declarado o no declarado tal, para hacerle firmar un documento que importe cualquier efecto jurídico, en daño de él o de otro, aunque el acto sea civilmente nulo;

3. El que defraudare usando de pesas o medias falsas;

4. El empresario o constructor de una obra cualquiera o el vendedor de materiales de construcción que cometiere, en ejecución de la obra o en la entrega de los materiales, un acto fraudulento capaz de poner en peligro la seguridad de las personas, de los bienes o del Estado;

5. El que cometiere fraude en perjuicio de alguna administración pública;

6. El que maliciosamente afectare el norma desenvolvimiento de un establecimiento o explotación comercial, industrial, agropecuaria, minera o destinado a la prestación de servicios; destruyere, dañare, hiciere desaparecer, ocultare o fraudulentamente disminuyere el valor de materias primas, productos de cualquier naturaleza, máquinas, equipos u otros bienes

[22] www.oas.org/dil/esp/codigopenal_de_la_republica_argentina.pdf

de capital (Inciso incorporado por el art. 2 de la Ley No. 25.602 B.O. 20/6/2002)

En los casos de los tres incisos precedentes, el culpable, si fuere funcionario o empleado público, sufrirá además inhabilitación especial perpetua (Párrafo sustituido por art. 3 de la Ley No. 25.602 B.O. 20/6/2002)

(Nota Infoleg: Por art. 4 de la Ley No 25.602 B.O: 20/6/2002) se incorporó el artículo 174 bis pero fue vetado por Decreto No. 1059/2002 B.O: 20/6/2002)"[23]

Artículo 175.- **"**Será reprimido con multa de mil pesos a quince mil pesos:

1. El que encontrare perdida una cosa que pertenezca o un tesoro y se apropiare la cosa o la parte del tesoro correspondiente al propietario del suelo, sin observar las prescripciones del Código Civil;
2. El que se apropiare una cosa ajena, en cuya tenencia hubiere entrado a consecuencia de un error o de un caso fortuito;
3. El que vendiere la prenda sobre que prestó dinero o se la apropiare o dispusiera de ello, sin las formalidades legales;
4. El acreedor que ha sabiendas exija o acepte de su deudor, a título de documento, crédito o garantía por una obligación no vencida, un cheque o giro de fecha posterior o en blanco.

(Nota Infoleg: multa actualizada por art. 1 de la Ley No. 24.286 B.O. 29/12/1993)"[24]

[23] www.oas.org/dil/esp/codigopenal_de_la_republica_argentina.pdf

[24] www.oas.org/dil/esp/codigopenal_de_la_republica_argentina.pdf

5.5. PERÚ

"En el ámbito penal, la Ley No. 27309 de 2000 modifica el Código Penal para sancionar algunos delitos informáticos. Así, se sanciona al que utiliza o ingresa indebidamente a una base de datos, a un sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para inferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos. Adicionalmente se castiga a quien altere, dañe o destruya una base de datos, un sistema, una red o un programa de computadoras. Asimismo, se establece una mayor penalidad si el agente accede a una base de datos, sistema o red de computadoras, haciendo uso de información privilegiada, obtenida en función a su cargo o pone en peligro la seguridad nacional."[25]

El Título V, Capítulo X del Código Penal Peruano dice a la letra:

DELITOS INFORMÁTICOS

Artículo 207 A.- "El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuentidós o ciento cuatro jornadas. Si el agente actúo con el fin de obtener un beneficio económico, será reprimido con pena privativa de la libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas."[26]

Artículo 207 B.- "El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma

[25] Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. Pg. 23

[26] www.oas.org/dil/esp/codigo_penal_perú.pdf.

con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres no mayor de cinco años y con setenta a noventa días multas."[27]

Artículo 207 C.- **"**En los casos de los Artículos 207 A y 207 B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:

1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de información privilegiada, obtenida en función a su cargo.

2. El agente pone en peligro la seguridad nacional."[28]

CAPITULO XI. DISPOSICIÓN COMÚN

Artículo 208.- **"**No son reprimibles, sin perjuicio de la repartición civil, los hurtos, apropiaciones, defraudaciones o daños que se causen:

1. Los cónyuges, concubinos, ascendientes, descendientes y afines en línea recta.

2. El consorte viudo, respecto de los bienes de su difunto cónyuge, mientras no hayan pasado a poder de tercero.

3. Los hermanos y cuñados, si viviesen juntos.

Posteriormente, a fines de septiembre del 2013 se aprueba "La Ley de Delitos Informáticos (Ley No. 30096), la cual fue criticada duramente.

Posteriormente, el presente año se promulga la Ley 30171 modificatoria a la Ley 30096 (Ley de Delitos Informáticos) en sus artículos 2, 3, 4, 5, 7, 8, y 10."[29]

[27] Ibid.

[28] Ibid

[29] www.oas.org/dil/esp/codigo_penal_perú.pdf

Referente al delito denominado "Fraude Informático" dice a la letra:

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 no mayor de ocho años y con setenta a ciento veinte días-multa.

La pena será privativa de libertad no menor delinco no 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"[30].

5.6. CHILE

"En materia penal la Ley No. 19223 sobre delincuencia informática (1993) tipifica los delitos de sabotaje informático, espionaje informático, alteración de datos, la revelación o difusión no autorizada de datos contenidos en un sistema."[31]

Con referencia al "Fraude Informático" (Artículo 468 bis del Código Penal) dice:

"Bajo el título de fraude informático se castiga a quien, valiéndose de cualquier manipulación informática (por ejemplo alterando indebidamente el funcionamiento de un sistema informático o los datos contenidos en el mismo) modifica una situación patrimonial en perjuicio de otro.

[30] Ibid.

[31] Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. Pg. 7

Esta conducta es sancionada con las penas de los delitos comunes de estafa, las que varían según el monto de lo defraudado. En concreto, ello significa penas de 61 días a 5 años de presidio, además de multa de 5 a 30 UTM (aprox. 200 a 1100 US)"[32].

5.7. ORGANISMOS INTERNACIONALES

a) Compromisos Internacionales en América Latina

"El Plan Regional eLAC 2007 plantea promover diálogos, intercambios y cooperación regional sobre experiencias nacionales en temas de ciberseguridad, spam y aspectos institucionales y tecnológicos relacionados. De igual forma incluye dentro de sus metas el establecer grupos de trabajo subregionales para promover y fomentar políticas de armonización de normas y estándares con el fin de crear marcos legislativos que brinden confianza y seguridad, tanto a nivel nacional como a nivel regional, prestando especial atención a la legislación sobre delitos informáticos y delitos por medio de la Tic como marco para el desarrollo de la sociedad de la información."[33]

"De igual forma, estipula al alentar las iniciativas regionales existentes para integrar las TIC en los sistemas nacionales de justicia, tales como el Proyecto de Justicia Electrónica impulsado por las Cortes Suprema de justicia de los países iberoamericanos."[34]

[32] www.oas.org/dil/esp/codigo_penal_chile.pdf.

[33] Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. Pg. 43

[34] Ibid. Pg. 43

"En virtud del Plan Regional eLAC 2010 se invita a los países a estudiar la posibilidad de ratificar o adherirse al Trato de Ciberdelitos del Consejo de Europa y su Protocolo adicional, como un instrumento facilitador para la integración y adecuación normativa en esta materia, enmarcados en principios de protección de los derechos de privacidad."[35]

b) Instrumentos Internacionales

"El Tratado de Ciberdelitos del Consejo de Europa y su Protocolo Adicional abordan temas de derecho penal sustantivo y procesal, que obligan a los Estado Miembros a instrumentar medidas para incorporar sus disposiciones en las leyes nacionales, así como cuestiones de cooperación internacional.[36]

"En el ámbito sustantivo, la Convención incorpora cuatro categorías de delitos que conforman un listado mínimo con los ilícitos extraditables que se mencionan a continuación y establece los elementos de tipo penal que deben ser incluidos en su definición.

- Delitos contra la confidencialidad, la integridad y la disponibilidad de datos y sistemas informáticos: i) accesos ilícitos a un sistema informático; ii) interceptación ilícita de datos informáticos; iii) interferencia en los datos (daño, borrado o alteración); iv) interferencia del sistema (mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos); v) abuso de dispositivos (software o contraseñas para cometer delitos).

[35] Ibiod. Pg. 43

[36] Ibid. Pg. 43

- Delitos informáticos: i) falsificación informática, y ii) fraude informático.
- Delitos relacionados con el contenido; i) delitos relacionados con la pornografía infantil, y ii) delitos de xenofobia.
- Delitos relativos a la propiedad intelectual y derechos afines."[37]

"Tanto la Unión Internacional de Telecomunicaciones (UIT), como la OCDE, APEC y la OEA han promovido dentro de sus agendas diversas actividades para promover la seguridad en línea y la capacitación a diversas autoridades administrativas, judiciales y parlamentarias en temas relacionados con los delitos informáticos. El programa sobre Ciberseguridad para apoyar a los países en desarrollo para 2007 a 2009 de la UIT, las Directrices de la OCDE para la Seguridad de los Sistemas Informáticos y de las Redes – Hacia una Cultura de la Seguridad (2002), así como el Proyecto de capacitación para Jueces y Fiscales en materia de Ciberdelitos de APEC (2005-2008) y los trabajos de Grupo Relator sobre Ciberseguridad e Infraestructura Crítica de CITEL, evidencia algunos avances en la materia"[38].

"Los delitos comúnmente sancionados son la interceptación de comunicaciones, el espionaje informático, el acceso ilícito a los sistemas de cómputo, el daño informático, el sabotaje informático, el fraude por medios electrónicos, la falsificación de documentos electrónicos o informáticos, la interrupción de comunicaciones, la supresión o alteración de pruebas digitales, la revelación o difusión no autorizada de datos contenidos en un sistema informático, la pornografía infantil haciendo uso de medios electrónicos, así como la violación de los derechos de propiedad intelectual e escala comercial."[39]

[37] Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. Pg. 44

[38] Conferencia de las Naciones Unidas sobre Comercio y Desarrollo. Pg. 44

[39] Ibid. Pg. 45

Es necesario señalar como corolario que como observamos anteriormente, existen varios países latinos que ya cuentan con normativa adecuada a la realidad tecnológica actual y que Bolivia, en la actualidad, se encuentra resagado debiendo tomar las medidas pertinentes para ir de la mano con el desarrollo de las nuevas tecnologías.

CAPITULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES

De acuerdo a lo analizado a lo largo del presente trabajo se llega a las conclusiones que se detallan a continuación:

- **PRIMERO**.- Como consecuencia del desarrollo de la Informática en todos los campos de la vida cotidiana, ya sea a nivel laboral como recreacional surgen diferentes tipos de actividades ilícitas, mismas que se manifiestan de formas inimaginables afectando de esta manera a un conjunto de bienes jurídicamente protegidos. Siendo una de las más comunes la denominada "Estafa Electrónica" o "Fraude Informático" y teniendo la necesidad imperiosa de una correcta regulación debido a que este tipo de conductas gozan de cierta impunidad en nuestra sociedad.

- **SEGUNDO**.- Existe una infinidad de hechos delictivos cometidos mediante la manipulación de computadoras, a saber la manipulación de datos de entrada, manipulación de programas, manipulación de datos de salida, fraude efectuado por manipulación informática, conductas delictivas en los instrumentos de pago como la clonación y falsificación de tarjetas, captación y uso indebido de datos y las conductas derivadas de la utilización de estos instrumentos de pago, mismas que se constituyen en "Estafa Electrónica", hechos descritos anteriormente y que merecen ser tipificados y sancionados en la vía penal.

TERCERO.- El Código Penal Boliviano, no obstante de no estar exento de la problemática actual, al abordar en el Capítulo XI la tipificación y penalización de delitos informáticos, no contempla la descripción de las conductas delictivas

detalladas a lo largo del trabajo de investigación, lo cual debilita la lucha contra estos ilícitos denominados "Delitos Informáticos". Por consiguiente, la atipicidad de las mismas en nuestro ordenamiento jurídico penal vigente imposibilita una calificación jurídico-legal que individualice a las mismas, llegando a existir una alta cifra de criminalidad e impunidad, haciéndose imposible sancionar como delitos, hechos no descritos en la legislación penal ya que se estaría violando el principio de legalidad expreso en la máxima "Nullum crime sine lege". En consecuencia es altamente positivo tipificar como delito la "Estafa Electrónica".

CUARTO: De los hechos descritos se llega también a la conclusión de que nuestro Estado Plurinacional se encuentra rezagado en la tipificación penal relativa a los delitos informáticos, especialmente en la "Estafa Electrónica" porque no cuenta con un cuerpo normativo integral y diversificado para todas las áreas que hoy debieran estar reguladas como las diferentes formas de delitos por Internet o las acciones delincuenciales a través de las redes sociales como el Facebook y Twitter.

QUINTO: En nuestra sociedad, aunque la Ley demuestra un avance significativo en la atención legislativa al problema, se hace imperativo armonizar las medidas judiciales, legislativas y policiales a través de capacitaciones que permitan enfrentar adecuadamente tan importante fenómeno de la criminalidad informática.

SEXTO: Los diferentes tratados internacionales y la legislación comprada, que hacen énfasis a los delitos informáticos son un recordatorio para que cada Estado cuente con una adecuada legislación para de esta manera poder sancionar este tipo de delitos.

6.2. RECOMENDACIONES

- Revisar las normas penales, su aplicación, vacios y carencias para de esta manera proponer las reformas legislativas que correspondan, con el fin de brindar seguridad laboral para aquellas personas a quienes ésta destinada la red y para poder tener un marco legal debidamente diseñado que llene las expectativas de toda nuestra sociedad.

- Es fundamental, educar y enseñar a la población boliviana sobre el uso correcto de las herramientas informáticas y las conductas prohibidas con el fin de protegerse y no convertirse en un agente de dispersión que pueda contribuir a propagar por ejemplo un virus.

- Es imprescindible la creación de órganos de protección contra este tipo de delitos y más gente especializada en el tema con una capacitación permanente que ayude a crear políticas de seguridad dirigidas a asegurar la integridad, disponibilidad y confidencialidad de los sistemas informáticos.

- Es necesaria la cooperación entre los diversos países para combatir con estas figuras delictivas que hoy en día se convierte en un fenómeno mundial.

- Como en todos los países del mundo, no estamos exentos a sufrir cualquier tipo de delito informático. Hablando de la "Estafa Informática" y su constante incremento dentro de nuestra sociedad, se debe fortalecer y proteger la seguridad e integridad de la información en las diferentes organizaciones de manera conjunta con profesionales informáticos para de esta manera poder combatir y prevenir este tipo de delitos.

PROYECTO DE LEY

EXPOSICIÓN DE MOTIVOS

La Constitución Política del Estado Plurinacional de fecha 7 de febrero de 2009, en su Titulo II, referido a los derechos reconocidos por la Constitución, establece que estos son inviolables, universales, interdependientes, indivisibles y progresismos. El estado tiene el deber de promoverlos, protegerlos y respetarlos.

Asimismo la misma Constitución Política del Estado Plurinacional de Bolivia, en su Capítulo dedicado a los Derechos Civiles y Políticos, establece en el artículo 21, numeral 2 que:

Las bolivianas y los bolivianos tienen los siguientes derechos: "A la privacidad, intimidad, honra, honor, propia imagen y dignidad".

En su sección IV, dedicado a Ciencia, Tecnología e Investigación, establece en el artículo 103 que:

I. El Estado garantizará el desarrollo de la ciencia y la investigación científica, técnica y tecnológica en beneficio del interés general. Se destinarán los recursos necesarios y se creará el sistema estatal de ciencia y tecnología.
II. El Estado asumirá como política la implementación de estrategias para incorporar el conocimiento y aplicación de nuevas tecnologías de información y comunicación.
III. El Estado, las universidades, las empresas productivas y de servicio públicas y privadas y las naciones y pueblos indígena originario campesinos, desarrollarán y coordinaran procesos de investigación, innovación, promoción, divulgación, aplicación y transferencia de ciencia y tecnología para fortalecer la base productiva e impulsar el desarrollo integral de la sociedad, de acuerdo con la ley.

En el tema de legislación de los delitos informáticos en Bolivia, **el CÓDIGO PENAL BOLIVIANO** solo prevé dos delitos, de los 15 delitos establecidos por la ONU-OMPI. Se tiene Manipulación Informática y Acceso Indebido dentro del Código Penal.

En el capítulo IV que hace referencia a las estafas y otras defraudaciones, establece en el artículo 335 que:

El que con la intención de obtener para sí o un tercero un beneficio económico indebido, mediante engaños o artificios provoque o fortalezca error en otro que motive la realización de un acto de disposición patrimonial en perjuicio del sujeto en error o de un tercero, será sancionado con reclusión de uno (1) a cinco (5) años y con multa de sesenta (60) a doscientos (200) días.

Es deber de la Asamblea legislativa Plurinacional, legislar las normas y/o adecuarlas a la realidad que vive el Estado para lo cual es necesario adecuar las normas legales que rigen la materia.

ANALISIS

I. Como consecuencia del avance tecnológico de la Informática, se observa un incremento inconmensurable de conductas antijurídicas tales como la "Estafa Electrónica", misma que implica responsabilidad para aquellos que la cometen y a la ausencia de una ley aplicable a este tipo de delitos denominados "Informáticos" utilizando como instrumento o medio la red de Internet, ha ce que exista la necesidad de tipificarlos y penalizarlos en Bolivia.

II. La legislación boliviana debe adecuarse a los cambios y a la evolución de la sociedad para de esta manera poder realizar un correcto tratamiento de las distintas formas antijurídicas informáticas. Es imperativo que la Tecnología de

la Información y Comunicación sea regulada de forma tal que no exista tanta inexactitud dentro del ámbito jurídico y, de esta manera exista un mejoramiento en cuestiones de seguridad informática, no solamente al referirnos a la parte técnica, sino también a las consecuencias que puedan llevar consigo la violación de las mismas dentro del ámbito jurídico.

III. El Derecho Penal de los Estados interesados en combatir esta nueva delincuencia, contienen vacíos jurídicos y diferencias importantes susceptibles de obstaculizar la lucha contra la delincuencia organizada y el terrorismo, así como los graves ataques contra sistemas de información perpetrados por particulares. La aproximación del Derecho Positivo en materia de delincuencia informática contribuirá a que las legislaciones nacionales sean lo suficientemente completas para que todas las formas de ataque contra los sistemas de información puedan ser objeto de investigación mediante técnicas y métodos disponibles en Derecho Penal.

Por lo anteriormente expuesto, se recomienda la aprobación del presente Proyecto de Ley.

PROYECTO DE LEY DE COMPLEMENTACIÓN DEL CÓDIGO PENAL BOLIVIANO

Por cuanto, la Asamblea Legislativa Plurinacional, ha sancionado la siguiente Ley:

LA ASAMBLEA LEGISLATIVA PLURINACIONAL

DECRETA:

ARTICULO 1°.- (OBJETO). *La presente ley tiene por objeto complementar los delitos informáticos cometidos por personas en su aplicación y procedimiento en lo que se refiere a la estafa electrónica.*

ARTÍCULO 2°.- (FINALIDAD). *La finalidad de la presente Ley consiste en sancionar los delitos informáticos en lo que se refiere a la estafa electrónica.*

ARTÍCULO 3°.- (COMPLEMENTACIÓN). *Inclúyase en el artículo 363 de la ley Nº 1768 de fecha 18 de marzo de 1997 - Código Penal Boliviano, la complementación, debiendo quedar en la forma siguiente:*

ARTÍCULO 363º (CUATER).- (ESTAFA INFORMATICA).- Todo aquel que, a través del uso indebido de tecnologías de información, valiéndose de alguna manipulación informática o artificio semejante, consiga insertar instrucciones falsas o fraudulentas, que produzcan un resultado que permita obtener un beneficio económico en perjuicio ajeno, será sancionado con reclusión de tres a siete años y multa de sesenta a doscientos días.

Remí*tase al órgano Ejecutivo, para fines Constitucionales*

Es dada en la sala de asamblea Legislativa Plurinacional, a los veintisiete días del mes de septiembre del año dos mil catorce

Fdo….

Por tanto, la Promulgo para que se tenga y se cumpla como Ley del Estado Plurinacional de Bolivia.

Palacio de Gobierno de la ciudad de La Paz, el primer día del mes de octubre del año dos mil catorce.

.

(Fdo. JUAN)EVO MORALES AYMA

PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

BIBLIOGRAFIA

- ARCE JOFRÉ, Jofré
  "Informática y Derecho"
  Ediciones Instituto Boliviano de Investigaciones Jurídicas, La Paz, 2013.
- AZPILCUETA, Hermilio Tomás
  "Derecho Informático"
  Editorial Abeledo-Perrot, Buenos Aires, 1987.
- CABANELLAS DE TORREZ, Guillermo
  "Diccionario Jurídico Elemental"
  Editorial Heliasta S.R.L., 1993
- CANO, Jeymi J.
  "Comerico Electrónico"
  Legis Editores S.A., Colombia, 2005.
- CORREA, Carlos M.
  "Derecho Informático"
  Ediciones de Palma, Buenos Aires, 1987.
- DAVARA RODRIGUEZ, Marco Antonio
  "Manual de Derecho Informático"
  Editorial Avanzadi, 10ma. Edición, Madrid, 2008
- GUIBOURG, Ricardo
  "Fenómeno Normativo: Acción, Norma y sistema, La Rev. Informática, Niveles de Análisis Jurídico".
  Astrea, buenos Aires, 1987.
- GUSTAVINO, Elías P.
  "Responsabilidad Civil y otros Problemas Jurídicos en Computación"
  Ediciones la Rocca, Buenos Aires, 1987.

- HERNÁNDEZ SANPIERE, Roberto. FERNANDEZ COLLADO, Carlos. BAPTISTA LUCIO, Pilar
  "Metodología de la Investigación"
  MC Graw-Hill Interamericana, 3ra. Edición, México, 2002.
- MORENO NAVARRETE
- MORENO NAVARRETE, Miguel Ángel
  "Contratos Electrónicos"
  Marcial Pons, Madrid, 1999.
- NACIONES UNIDAS
  "Estudio sobre las Perspectivas de la Armonización de la Ciberlegislación en América Latina".
  Conferencia de las Naciones Unidas sobre Comercio y Desarrollo, Nueva Cork y Ginebra, 2009.
- NAVARRO ISLA, Jorge
  "Tecnologías de la Información y de las Comunicaciones: Aspectos Legales"
  Editorial Porrua/Instituto Tecnológico Autónomo de México, 2005
- PEGUERA POOH, Miguel
  "Derecho y Nuevas Tecnologías"
  Editorial UOC, Barcelona, 2005.
- POSADA MAYA, Ricardo
  "Aproximación a la Criminalidad Informática en Colombia"
  Revista de Derecho, Comunicaciones y Nuevas Tecnologías, ediciones Uniandes, Bogotá, 2006.
- RICO CARRILLO, Mariliana
  "Los Desafíos del Derecho Penal frente a los Delitos Informáticos y otras Conductas Fraudulentas en los Medios de Pago electrónicos"
  IUS Revista del Instituto de Ciencias Jurídicas de Puebla, México, 2013.
- RIBAS ALEJANDRO, Javier

"Aspectos Jurídicos del Comercio Económico en Internet"
Avanzadi Editorial S.A., Pamplona, 1999
SUÑE LLINAS, Emilio
"Tratado de Derecho Informático"
Universidad Complutense, Madrid, 2006.

- TAMAYO TAMAYO, Mario
  "El Proceso de la Investigación Científica"
  Editorial Limusa S.A., 3ra. Edición, México D.F., 1996.
- TELLEZ VALDES, Julio
  "Derecho Informático"
  Interamericanas Ediciones S.A., 3ra Edición, México, 2004.
- VIEGA, María José
  "Protección de Datos y Delitos Informáticos"
  Revista de Derecho Informático, Perú, 2003.
- VILLABELLA ARMENGOL, Carlos Manuel
  "La Investigación y la Comunicación Científica en la Ciencia Jurídica"
  Instituto de Ciencias Jurídicas de Puebla, Primera Edición, México, 2009.
- CONSTITUCIÓN POLÍTICA DEL ESTADO PLURINACIONAL DE BOLIVIA
  Aprobada por Referéndum de 25 de enero de 2009, promulgada el 7 de febrero de 2009.
- CODIGO PENAL BOLIVIANO
  d.s. 0667
- LEY GENERAL DE TELECOMUNICACIONES, TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
  Ley 164, 8 de agosto de 2011.

REFERENCIAS ELECTRÓNICAS

- Acurio del Pino, "Delitos Informáticos: Generalidades" (en línea): http://www.oas.org/jurídico/spanish/cyb_ecu_delitos_inform.pdf (consulta 05/09/2014)
- Rojas, Raúl (1998). «How to make Zuse's Z3 a universal computer» (en inglés). *IEEE Annals of the History of Computing* **20**: pp. 51–54.(Consultado 23/11/14).
- http:/es.wikipedia.org/wiki/derecho_informático
- www.delitosinformaticos.com/estafas/delito.shtml.
- www.portaley.com/delitosinformaticos.thm.
- www.oas.org/dil/esp/codigo_penal_colombia.pdf.
- www.oas.org/dil/esp/codigopenal_venezuela.pdf.
- www.informaticajur.com/trabajos/criminalidad_informatica_en_bolivia. esp.
- www.bibliotecadigital.umsa.bo.
- www.oas.org/dil/esp/codigo_penal_peru.pdf.
- www.oas.org/dil/esp/codigo_penal_chile.pdf.
- www.oas.org/dil/esp/codigopenal_de_la_republica_argentina.pdf.
- www.unifr.ch/ddp1/derecho penal/legislacion/1_20080616_75.pdf.
- www.oas.org/juridico/spanish/mesicic3_ven_anexo6.pdf.
- www.ibered.org/legislación-codigo-penal.
- Htttp://pcolorador.blogspot.com/2008/04/delitosinformaticos_14htm.
- http:/es.wikipedia.org/wiki/penal
- http://www.cad.com.mx/que_es_internet.htm.
- www.perucontable.com
- es.wikipedia.org/wiki/manipulación