UNIVERSIDAD MAYOR DE SAN ANDRES
FACULTAD DE DERECHO Y CIENCIAS POLITICAS
CARRERA DE DERECHO
INSTITUTO DE INVESTIGACIONES Y SEMINARIOS

TESIS DE GRADO

“ EL FRAUDE INFORMATICO Y SU INCORPORACION EN EL CODIGO PENAL BOLIVIANO”

(Tesis para optar el grado de licenciatura en derecho)

Postulante: Rafael Roly Fernández Goyzueta

Tutor: Dr. Roberto Fernández Daza

LA PAZ – BOLIVIA

2012

DEDICATORIA

A Dios porque siempre hubo una luz después de una tormenta, pero en especial a mis Padres que de manera indirecta siempre me apoyaron y supieron alentarme en todo momento y situación para el desarrollo de mi vida, a pesar de todos los malos momentos que les hice pasar, pero siempre estuvieron firmes y persistentes fortaleciéndome cada día mas, enseñándome, que no se sale adelante celebrando éxitos, sino superando fracasos.

AGRADECIMIENTOS

A mi Tutor, que me fue asignado, por su paciencia y sus ganas de enseñar a la nueva generación de Abogados.

A las Autoridades que recurrí para que con su colaboración pueda realizar una mejor tesis.

A L.S.S.M. por siempre estar cuando te necesitaba ya que sin tu colaboración no podría haber terminado este proyecto.

RESUMEN ABSTARCT

EL FRAUDE INFORMATICO Y SU INCORPORACION EN EL CODIGO PENAL BOLIVIANO

El Fraude Informático puede constituir una amenaza a la estabilidad financiera y principalmente a la seguridad de Instituciones Públicas o Privadas y también a personas naturales que hoy en día no pueden estar aisladas de las nuevas tecnologías que trae la informática, pues a través de redes se pueden manejar una gran cantidad de dinero, como por ejemplo la banca por Internet, el pago de sueldos a través de cajeros automáticos, compras y ventas por Internet, etc. Por ello surge la necesidad de regular el desarrollo y aplicación de los sistemas informáticos relacionados con los movimientos económicos financieros para constituir normativas jurídicas que permitan luchar contra el Fraude Informático.

En el análisis y diagnostico de la problemática se llega a determinar que el Fraude Informático causa gran perjuicio a la sociedad Boliviana, ya que sus efectos alcanzan a personas naturales y jurídicas que necesitan usar los sistemas informáticos para su cotidiano vivir, y como es de esperarse nuestra legislación no puede combatir esto ya que en nuestra legislación rige el Principio NULLUM CRIME SINE LLEGUE, y por la atipicidad de la norma esta seria insancionable.

Las propuestas del estudio sugieren la aplicación de una norma penal para combatir el Fraude Informático en sus distintas variedades, pues este tipo de delitos solamente se pueden combatir con normas sancionadoras, y como se demuestra en la parte metodológica de la investigación también hay que tomar en cuenta las directrices de la corriente estructuralista del Derecho, donde se tiene que ver la relación ***Delito - Delincuente*** *ya que no cualquiera puede ser un delincuente informático, pues el perfil de este tipo delincuente es: que es de clase media, tiene estudios superiores, y tiene mucho conocimiento en*

Informática, por ello este delincuente informático comprendería exactamente el castigo que se le impondría si comete un Fraude Informático, si este estuviera claramente tipificado en el Código Penal.

Finalmente la presente Tesis de grado propone ante la instancia pertinente el anteproyecto de Ley que incorpora en el Código Penal Boliviano en el Capitulo XI, referido a los ***DELITOS INFORMATICOS****, después de los Arts. 363 bis y 363 ter, incluyendo como algo novedoso pero no extraño el Art. 363 quater. (FRAUDE INFORMATICO)*

EL FRAUDE INFORMATICO Y SU INCORPORACION EN EL CODIGO PENAL BOLIVIANO

INDICE GENERAL

PAG.

DESARROLLO DEL DISEÑO DE PRUEBA

CAPITULO III

MARCO TEORICO

CAPITULO IV

MARCO JURIDICO

DISEÑO DE LA INVESTIGACION

1. ENUNCIADO DEL TEMA

EL FRAUDE INFORMATICO Y SU INCORPORACION EN EL CODIGO PENAL BOLIVIANO

2. IDENTIFICACION DEL PROBLEMA

El creciente y significativo avance que ha generado el desarrollo, difusión y uso generalizado de la informática y su reciente impacto en la sociedad boliviana, despierta con la explosiva incorporación del Internet, que de modo inexorable está presente en todos los ámbitos del quehacer humano, revolucionando los patrones de comportamiento y por ende las relaciones sociales, jurídicas, políticas y económicas.

Estas nuevas relaciones humanas las cuales son producto de la informática, tiene una doble cara, ya que además de hacer la vida mas fácil para el ser humano, no está exenta de vicios y delitos los cuales surgen como nuevas figuras delictivas que la legislación penal boliviana no está preparada para combatir; Es así que la disciplina del Derecho se halla hoy en una instancia histórica en la que debe responder a estos nuevos y complejos problemas a los que se enfrenta. Por otra parte, la inexistencia de una legislación penal adecuada, posibilita al mismo tiempo, la impunidad y desprotección jurídica de la sociedad en general.

Por lo cual el presente trabajo de investigación tiene la finalidad de explicar a los lectores lo que en realidad es el FRAUDE INFORMATICO como una nueva figura delictiva creada gracias a la incorporación de la Informática en el país y al mismo tiempo se propondrá una modificación e incorporación de este nuevo

delito a la Legislación Penal Boliviana a través del Derecho Informático y el Derecho Penal, en este sentido, el Sistema penal Boliviano tendrá legitimación para privar de libertad al agente, solo en tanto y cuanto sea respetado el Principio de Legalidad, limitador del poder punitivo Estatal, debiendo previamente ser determinada la acción criminosa como comportamiento ilícito y ser legalmente reprimida a través de legislación penal.

3. PROBLEMATIZACION

Los aspectos anteriormente señalados, permiten formular el problema de investigación de la siguiente manera:

- ¿Sera que en Bolivia el fraude Informático llego a surtir perjuicios a la sociedad?
- ¿Es nuestra Legislación penal eficaz para combatir el fraude Informático?
- ¿Qué bien jurídicamente protegido es vulnerado por el Fraude Informático?
- ¿Sera que en el país existen denuncias sobre Fraude Informático y si existiesen en qué estado están y como se resolvieron?

4. DELIMITACION DEL TEMA DE LA TESIS

4.1 DELIMITACION TEMATICA

El tema de investigación se enmarca en el Derecho Informático por tratarse de un tema relacionado con la Informática y el Derecho Penal por ser una investigación de tipo propositiva de una norma a ser incorporada en el Código Penal Boliviano.

4.2. DELIMITACION TEMPORAL

El estudio de la investigación ha definido un periodo de análisis entre los años entre los años 2010 al 2011, esto porque los delitos del Fraude Informático datan de fechas relativamente actuales.

4.3 DELIMITACION ESPACIAL

La investigación fue realizada en la ciudad de La Paz, como epicentro urbano tecnológico del país, pero enfocando una dependencia más acertada para el buen desarrollo de la investigación el Ministerio Publico de La Paz, oficinas de la FELCC, Juzgados Penales, etc.

5. FUNDAMENTACION E IMPORTANCIA DEL TEMA DE LA INVESTIGACION

El objetivo fundamental de la investigación tiene como referencia al creciente avance que ha generado el desarrollo, difusión y uso generalizado de la informática y su reciente impacto en la sociedad boliviana que despierta con la explosiva incorporación del **Internet**, que de modo violento está presente en todos los ámbitos del quehacer humano, revolucionando los patrones de comportamiento y por ende las relaciones sociales.

El uso de estos sistemas informáticos a generado múltiples actividades en los mercados, ha posibilitado al entorno empresarial como a particulares en general, hacer uso de modernos servicios del Internet tanto en publicidad con el uso de páginas web, obtención de comunicación efectiva, dinámica e instantánea y a escala mundial con el uso de direcciones electrónicas, así como

la aplicación cada vez más frecuente del comercio electrónico, tiendas virtuales y empleo de contratos informáticos entre personas naturales y jurídicas.

Como es una nueva forma de conexión en el mundo, no está exento de delincuencia, ya que en la actualidad se han formados expertos virtuales, llamados delincuentes informáticos, que usan a este flujo de información para delinquir.

Así es el caso del llamado “Fraude Informático” que es aquella conducta consistente en la manipulación de datos, alteración o procesamiento de datos falsos contenidos en el sistema informático, realizada con el propósito de obtener un **beneficio económico**. Hay muchos tipos de Fraude Informático entre ellos tenemos al uso de los caballos de Troya ¨trojan hourses¨, el cual es un programa informático destinado a introducir rutinas o instrucciones aparentemente inicuas, para distorsionar el funcionamiento del sistema y así cometer fraudes vía internet, como también a través de la técnica del salami ¨rounding down¨ la cual permite sustraer mediante redondeo, pequeñas cantidades de activos financieros de diversas cuentas bancarias para situar su monto total, que puede ascender a cantidades considerables, en la cuenta del delincuente informático o “Hacker”.

Entonces el objetivo fundamental de la presente investigación es la de introducir este nuevo delito como es el “FRAUDE INFORMATICO” en el Código Penal Boliviano, para así tener una mejor aplicabilidad del Derecho y dotar de armas legales a los encargados de impartir justicia en nuestro país para que apliquen una buena subsunción de este delito y no caer en la atipicidad de la norma cuando este tipo de hechos delincuenciales sean cometidos.

6. OBJETIVOS DEL TEMA DE INVESTIGACION

6.1. Objetivo General

- Proponer un proyecto de ley para incorporar el Fraude lnformático en el código penal Boliviano para tipificar este tipo de conductas delictivas.

6.2. Objetivos Específicos.-

- Determinar si el fraude informático está tipificado en el código penal boliviano.

- Analizar qué tipo de fraude informático se cometen con mayor frecuencia en la ciudad de la Paz.

- Determinar qué bien jurídico vulnera el delito del Fraude Informático y comparar teóricamente la legislación boliviana con la extranjera, en materia de sanciones y penalidades en lo respecto al delito del fraude informático.

7.- HIPÓTESIS DE TRABAJO

“La tipificación del "Fraude informático" en el código penal boliviano, permitirá prevenir los desfalcos, extorsiones, hurtos de cuentas, transferencias ilegales de dinero, etc. para así lograr seguridad en el manejo de las redes informáticas.”

8. VARIABLES DE LA INVESTIGACIÓN

8.1. Variable Independiente

- La tipificación del "Fraude informático" en el código penal boliviano.

8.2. Variables Dependiente

- prevenir los desfalcos, extorsiones, hurtos de cuentas, transferencias ilegales de dinero.
- lograr seguridad en el manejo de las redes informáticas.

9. METODOS QUE FUERON UTILIZADOS EN LA INVESTIGACION

La presente investigación se enmarca en los siguientes Métodos

Método Deductivo-inductivo.- Es un razonamiento que va de lo general a lo particular y a la inversa, ambos métodos nos ayudaran a profundizar el tema del Fraude Informático que no tiene pena y escasamente está tipificado, lo cual a criterio del autor de la presente investigación da a conocer uno de los puntos débiles de la legislación boliviana pues su impacto ya ha causado gran conmoción en la sociedad boliviana.

El Método Jurídico.- Este método nos permite una aproximación al fenómeno jurídico en su realidad histórica, humana y social, además nos permite interpretar las normas jurídicas vigentes en el ordenamiento jurídico interno en el país referente a los delitos informáticos en especial el fraude informático.

Método Teleológico.- Este método nos permitirá encontrar el interés jurídicamente protegido para que la investigación tenga un respaldo jurídico.

Método Analógico Comparativo.- Este método nos permitirá realizar una comparación de Nuestra legislación con otras legislaciones extranjeras y de esa manera observar y analizar, como otros países tipifican clara y concretamente estos nuevos delitos informáticos, pues este tema es de nivel mundial.

10. TECNICAS QUE FUERON UTILIZADAS EN LA TESIS

La técnica empleada en el presente trabajo, se ha centrado en el ámbito de la recolección de datos bibliográficos, realización de fichas de trabajo basada en la corriente de la escuela estructuralista del derecho, sobre delito – profesión o estatus social, finalmente a efectos de validar los resultados hallados se recurrió a la técnica de la entrevista a expertos en la materia.

DESARROLLO DEL DISEÑO DE LA PRUEBA

INTRODUCCION

El siglo XX se ha distinguido por la revolución tecnológica, actualmente los sistemas informáticos están presentes en casi todos los campos de la vida moderna, actividades personales, comerciales, etc., 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, viéndose facilitado por el uso de la red Internet, que hace unos años solamente se podían obtener tras largas horas de búsqueda en bibliotecas; en cambio hoy se puede conseguir la información deseada en cuestión de minutos, asimismo se puede procesar, seleccionar, transmitir mediante procedimientos sencillos, por lo que se puede afirmar que vivimos en la denominada “Sociedad de la Información”.

El auge de las telecomunicaciones y el surgimiento de las redes informáticas, ha conducido que existan nuevas formas de interrelacionarnos con nuestros semejantes que podrían encontrarse a miles de kilómetros de distancia, como ser el Facebook, e-mail, chat, foros, etc., fenómeno mundial que otorga grandes beneficios, sin embargo de la misma manera ofrece un aspecto negativo cuando personas inescrupulosas, con mala voluntad o negligentes lo utilizan como instrumento para el cometido de su accionar en detrimento de los demás, es así que conductas antisociales tradicionales se manifiestan en formas no tradicionales, planteando problemas en cuanto al funcionamiento y seguridad de los sistemas informáticos, toda vez que la informática reúne características que la convierten en un medio idóneo para la comisión de distintas modalidades delictivas, la manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos, el acceso y la utilización indebida de la

información que puede afectar la esfera de la privacidad, con la finalidad de obtener grandes beneficios económicos o causar importantes daños materiales o morales.

Es indudable que la informática incita la imaginación de las personas, asimismo otorga confianza, impunidad debido a que éstas conductas son de difícil descubrimiento y que muchas instituciones públicas o privadas que se ven afectadas no llegan a denunciarlas por las secuelas que acarrearían ante la vulnerabilidad de su sistema informático.

La propagación de la Internet y el mayor uso de la tecnología plantea nuevos desafíos, sumado al desarrollo del comercio electrónico y la dependencia de la sociedad frente a la tecnología, es necesario la utilización de políticas de seguridad como el uso del cifrado, las firmas digitales, control de acceso, uso de firewalls, asimismo medios jurídicos prácticos y eficaces para prevenir diversas actividades delictivas.

La importancia de una regulación jurídica se basa en que la delincuencia informática se comete en el ciberespacio, no reconoce las fronteras nacionales convencionales, puede perpetrarse desde cualquier lugar y contra cualquier usuario del mundo, por lo que se necesita a nivel nacional respuestas prontas, lo que no implica que se circunscriba a nivel interno sino más bien con políticas internacionales de lucha frente a estos nuevos retos de seguridad en la red y la delincuencia informática; toda vez que se verá entorpecida si existen una diversidad de legislaciones en cuanto a su tratamiento y penalización, sumado a la ausencia de tratados de extradición.

A nivel internacional se han realizado convenciones, congresos que sugieren una legislación análoga para una lucha eficaz, debiendo los países poner mayor énfasis en la lucha contra la pornografía infantil en la red y demás delitos

cibernéticos incluyendo el Fraude Informático que es la base de la presente investigación.

La delincuencia informática como fenómeno de la era tecnológica se caracteriza por su carácter transnacional, dificultad de descubrimiento e impunidad. Entre las conductas cometidas por delincuentes informáticos; tenemos como base de nuestra investigación al fraude a través de sistemas informáticos, en la economía actual la información es una parte vital, más aún ante el creciente desarrollo del comercio online pero ante la inseguridad de los usuarios online, su consiguiente impacto en toda actividad humana se da por que no existe una protección jurídica adecuada, idónea a la realidad social y tecnológica en que vivimos, sumado al carácter especial de las conductas que no admiten encuadrarse dentro de figuras convencionales, siendo necesaria la creación de nuevas figuras penales tomando en cuenta la validez de la información contenida en los bancos de datos y el perjuicio que pudieran ocasionar.

En nuestro país si bien se ha insertado dos artículos relacionados a delitos informáticos, los legisladores no han creado un organismo policial especializado para la investigación de este tipo de delitos, incrementándose la inseguridad que tienen las personas, la creación de este organismo quedaría pendiente aun.

Viendo ésta problemática tecnológica actual, se ha tomado como objeto de estudio el FRAUDE INFORMÁTICO, base de la presente investigación, formulando como hipótesis de trabajo:

“La tipificación del "Fraude informático" en el código penal boliviano, permitirá prevenir los desfalcos, extorsiones, hurtos de cuentas, transferencias ilegales de dinero, etc. para así lograr seguridad en el manejo de las redes informáticas.”

En el Primer Capítulo se establece algunos de los precedentes que son de interés dentro de la presente tesis, conformando los antecedentes del presente estudio. Tales antecedentes están referidos primeramente a los orígenes tanto del Internet como de la Informática que están comprendidos dentro la relación del Fraude Informático y las comunicaciones en Bolivia.

En este capítulo se trata de explicar cuál es el origen de la comunicación a grandes rasgos para llegar a la comunicación de la era tecnológica, el origen y características del Internet y las formas de comunicación que se desarrollan a través de su red, tomando en cuenta que no toda invención es buena pues también puede traer peligro y confrontación si llega a manos criminales.

El Segundo capitulo tiene la finalidad de describir y desarrollar todo lo que tiene que ver con el fondo del tema, se determina los temas que tienen directa relación con el Fraude Informático es decir se determina lo que es el Derecho informático, los Delitos informáticos, los conceptos, teorías que tienen que ver con el tema, utilizando teorías, jurisprudencia, doctrina, etc., pero nunca apartándonos del tema principal, puesto que este capítulo es una especie de preámbulo para que el lector pueda entender mejor el fondo del asunto y no entorpecer la misma dirigiéndonos directamente a resolver el problema.

El Tercer Capítulo es la síntesis de lo que es el Fraude Informático y todos los tipos de fraude que se cometen por el internet y las redes.

Se describe una introducción teórica a todos los elementos centrales de la problemática de la presente tesis. Los cuales sirven al diagnostico de la realidad informática. Dichos elementos son los delitos informáticos y la teoría del fraude informático que viene a ser una conformación no caprichosa del destino, sino un conjunto de causas determinantes para la comisión del ilícito o en este caso la prevención del mismo.

El Cuarto Capítulo es el análisis del delito de fraude informático pero desde el punto de vista netamente jurídico ya sea penal o administrativo.

La visión holística del presente trabajo de tesis, nos coloca ante la necesidad de verificar el efecto de las normas actuales en la regulación del fraude informático y la suficiencia de la hipótesis con respecto a la variable interviniente jurídica.

En este análisis surge el requisito de establecer si es suficiente la regulación actual y corresponde al estudio de los vacíos jurídicos la tarea de determinar esta necesidad de regulación.

El capítulo igualmente responde a la finalidad de establecer los efectos que ha logrado la norma penal desde 1997, determinándose un estudio de casos de delitos informáticos en el ámbito nacional y realizar una comparación jurídica con los países vecinos acerca de su regulación normativa contra el fraude Informático.

El Quinto Capitulo esta enteramente dirigida a la demostración y comprobación de la Hipótesis planteada ya que se tuvo que realizar una serie de sondeos de encuestas y entrevistas a expertos en el área donde corroboraron esta comprobación en un alto porcentaje, ya que todos los entrevistados afirmaron que hace falta un tipo penal que penalice el fraude informático.

Finalmente basándome en la hipótesis planteada, se ha utilizado el método deductivo y el método jurídico al contrastar la legislación comparada también se ha utilizado el método Teleológico toda vez que este ayuda a seleccionar el bien jurídicamente protegido cuando se comete este tipo de delitos y por último el inductivo a través del análisis exhaustivo del tema tratando de sintetizar

conceptos tales que me lleven a determinar la necesaria implementación de una nueva modificación del Código Penal y su inserción como tipo penal el Fraude informático considerando agravantes en su caso.

Básicamente se utilizó la técnica de la entrevista orientado principalmente a conocer criterios de profesionales abogados, para que a través de su vivencia y experiencia profesional puedan dar mayores luces en relación a los delitos informáticos, a investigadores de la FELCC básicamente de la División de Económicos y Financieros que es la división que recibe este tipo de delitos. y así determinar cuáles son las dificultades que tienen que tropezar cuando realizan sus investigaciones por la falta de material adecuado, a ingenieros en sistemas sobre las políticas de seguridad y los controles que se deberían seguir prevención, detección y protección.

CAPITULO I
MARCO HISTORICO

1.1. ANTECEDENTES HISTORICOS DE LA INFORMATICA

Si bien se conocen versiones primitivas del Abaco hacia dos mil quinientos años antes de Cristo, en el Medio oriente el Abaco chino data de aproximadamente de mil doscientos años antes de Cristo, esto dio inicio a una serie de invenciones de maquinas aritméticas que mayormente eran utilizadas por comerciantes de la época que ayudaron a realizar operaciones matemáticas y encuadrar sus cuentas en sus negocios, las invenciones llegaron hasta el hito de la informática que es el año de 1857, año en el cual, el considerado padre de la informática Charles Babbage invento la primera calculadora y recibió la distinción como el inventor de la primera computadora digital y universal.

Babbage, también invento la Máquina analítica, que es una máquina calculadora mecánica, de la cual sólo se construyó una pequeña parte. Esta máquina analítica, aunque concebida mucho tiempo antes de que surgiese la tecnología electrónica, debía ser capaz de almacenar instrucciones, realizar operaciones matemáticas y utilizar tarjetas perforadas como sistema de almacenamiento permanente. No obstante estas tarjetas perforadas se usaron por todo el mundo y su aplicación fue dirigida para el aumento de la producción en toda la industria, las fabricas de telares, en el ferrocarril, el comercio, etc.

Mejor dicho estas tarjetas perforadas fueron la base para la invención de los computadores que hoy conocemos, y hoy en día llegaron a tal grado que su

aplicación es tan amplia y es utilizada en todo campo tanto en la industria, comercio, la banca, los sectores privados, públicos, en la administración de gobierno, también se aplica en la ciencia en la investigación, en la educación, etc.

El avance tecnológico de los últimos 50 años y más precisamente después de la segunda guerra mundial[1], sucede a un ritmo vertiginoso alcanzando índices y desarrollos espectaculares en las comunicaciones e informática, la amplia difusión de la tecnología informática ha llevado a las transformaciones de las estructuras industriales, los equipos de producción masiva como impresoras de periódico, fotografías, empacadoras, embotelladoras, ensamblado, armado y prueba de automóviles, se controlan y dirigen por computadoras mediante un sistema de producción robotizado[2], con lo que se logra mayor rapidez, precisión y calidad cada vez mayor por sus significativos reflejos en la evolución industrial, política, económica, social, cultural, etc. Su impacto se traduce en primer lugar en la modificación de procesos y métodos de trabajo en la industria, por otro lado se resalta el incremento más efectivo en la productividad y mayor precisión en la fabricación de todo tipo de productos. Hoy en día la maquina analítica a invadido casi toda actividad humana y por ello la sociedad en la que vivimos ha sido calificada como la “Sociedad de la Información”.

1.2. LA RED INTERNET Y SU ORIGEN

1.2.1. ORIGEN DE LA RED INTERNET

[1] N. del A.: En los últimos años se ha desarrollado una distinción radical entre ciencia y tecnología. Con frecuencia los avances científicos soportan una fuerte oposición, pero en los últimos tiempos muchas personas han llegado a temer más a la tecnología qua a la ciencia. Para estás personas, la ciencia puede percibirse como una fuente objetiva y serena de las leyes eternas de la naturaleza, mientras que estiman que las manifestaciones de la tecnología son algo fuera de control.

[2] Fernández Daza, Roberto, Derecho Informático, Pág. 7

A finales de los años sesenta es concebida la primera red denominada "ARPANET" en la Agencia para el desarrollo de Proyectos Avanzados de Investigación (ARPA, Advanced Research projects), que tenía la misión de conectar los ordenadores de diferentes instituciones militares[3] con el fin de que las comunicaciones no se interrumpieran si alguna de ellas era destruida, sino que solamente se perdiera un nodo (Nodo, en informática y redes de área local, un dispositivo conectado a la red capaz de comunicarse con otros dispositivos de la misma)[4], logrando que las comunicaciones estuvieran descentralizadas.

El año 1974 Vinton Cerf (Ingeniero Estadounidense), junto con Robert Kahn, publican "Protocolo para Intercomunicación de Redes por paquetes", donde especifican el diseño de un nuevo protocolo[5], el Protocolo de control de transmisión (TCP, Transmisión Control Protocol) que ya estaba fuera del ámbito estrictamente militar el cual se convirtió en el estándar aceptado. La implementación de TCP permitió a las diversas redes conectarse en una verdadera red de redes, es decir conectarse a Internet.

En 1983 ARPANET se separa de la red militar que la originó, de modo que ya sin fines militares se puede considerar esta fecha como el nacimiento de Internet, su expansión es enorme mejorando los servicios; en 1985 se termina el desarrollo del aún vigente protocolo para la transmisión de ficheros en Internet (FTP, File Transfer Protocol), basado en la filosofía de cliente-servidor.

En 1990 Tim Berners-Lee, investigador del Centro Europeo de Investigación Nuclear (CERN), crea una nueva manera de interactuar con Internet: El World

---

[3] N. del A.: Red informatizada de uso interno y privado, accedida de manera restringida por miembros de la institución.

[4] Microsoft ® Encarta ® 2008. © 1993-2007 Microsoft Corporación. Reservados todos los derechos.

[5] Protocolo es el conjunto de reglas que controlan el formato y significado de los paquetes intercambiados por entidades de par. Se usan los protocolos para implementar los servicios de la Red.

Wide Web (WWW) sistema con el cual el intercambio de información se da con mayor facilidad, asimismo la localización y obtención de datos en forma gratuita.

El World Wide Web fue aumentando más a fondo por otros que crearon software y tecnologías para hacerlo más funcional. Por ejemplo, Marc Andreesen creó un nuevo navegador llamado Mosaic en 1993, posteriormente dirigió al equipo que creó Netscape Navigator. Asimismo, Berners-Lee, creó las bases del protocolo de transmisión HTTP, el lenguaje de documentos HTML y el concepto de los URL.

En Septiembre de 1993 se inició el primer servidor Web en español. En estos momentos se aumenta la potencia de las redes troncales de EE.UU., y en 1994 se eliminan las restricciones de uso comercial de la red y el gobierno de EE UU. deja de controlar la información de Internet, constituyéndose 1995 como el año del gran "boom" de Internet, puede considerarse como el nacimiento de la Internet comercial, contando con aproximadamente 3.8 millones de nodos registrados y más de 30 millones de usuarios.

Internet es identificada por la mayor parte de usuarios como la gran autopista de la información. Así, la eficaz intermediación de Internet posibilita reconducir los incontenibles flujos de información y contribuye a que la "sociedad de la información" pueda efectivamente transformarse en "sociedad del conocimiento", como consecuencia de la posibilidad de extraer conocimientos útiles de la sobreabundancia de información.

Para Llaneza González, Internet es un sistema de comunicación transnacional que gracias a unos estándares comunes, usando tecnologías y redes de telecomunicación, permite el intercambio y la obtención de información mediante el uso de diversas modalidades de comunicación en línea (listas de

correos, USENET, chats, etc.) Internet es información, tecnología y una red física de telecomunicación.

1.2.2. LA RED INTERNET

Internet es una red mundial de comunicación que opera a través de miles de redes enlazadas y situadas en diferentes lugares, utiliza el protocolo TCP/IP [6](acrónimo de *Transmisión Control Protocol/Internet Protocol "*protocolo de control de transmisiones/protocolo de Internet"), el cual posibilita la transmisión de ficheros digitales o sistemas de información en forma prácticamente instantánea, empleando los recursos de comunicación existentes: cables, teléfonos, satélites u ondas radioeléctricas; como fenómeno socio-tecnológico está forzando la carrera por establecer una nueva infraestructura de información.

Es preciso señalar la diferencia existente entre la Red y la Web, la primera es una red de redes, básicamente hecho de PC's y cables que envían paquetes de datos a cualquier parte del mundo. El WWW (World Wide Web) cuya traducción literaria es "mundo ancho telaraña" es abstracto (imaginario) un espacio de información, donde las conexiones son uniones entre hipertextos; mediante este servicio, el usuario dispone de un fácil acceso a la información como ser documentos, sonidos, videos, información ofrecida por multitud de servidores repartidos por todo el mundo. La Web no podría existir sin la red y hace la red útil, ambos conceptos web y red definen a Internet[7].

1.3. INCURSIÓN DE LA INTERNET EN BOLIVIA

[6] Microsoft ® Encarta ® 2008. © 1993-2007 Microsoft Corporation. Reservados todos los derechos.

[7] Su producción debe estar basada en nomas de desarrollo del software, independientemente de la imagen o dentro del diseño que se desea exponer.

Bolivia cuenta con una extensión territorial de 1'098'581 Km2, y una población de cerca de 10.5 millones de personas, las telecomunicaciones han estado a cargo de cooperativas telefónicas con un monopolio local, los servicios nacionales e internacionales de larga distancia a cargo de ENTEL, ofreciendo los servicios de telefonía celular TELECEL (1991) que se convertiría más adelante en TIGO, ENTEL (1996), y a fines de 1999 VIVA NUEVATEL monopolios que concluyen con la aplicación de la Ley de Telecomunicaciones, ofreciendo hoy en día no solo de telefonía celular pues también ofrecen internet inalámbrico utilizando los conocidos módems internet (es un acrónimo de 'modulador/demodulador'. Se trata de un equipo, externo o interno, utilizado para la comunicación de computadoras a través de líneas analógicas de transmisión de voz y/o datos[8]), dándose la apertura de mercados para un mejor servicio a precios competitivos.

El proceso de la incursión de Internet en Bolivia, se dio bajo el Programa Regional RLA/031/88 de la Oficina Regional para América Latina y el Caribe del Programa de Naciones unidas para el Desarrollo, constituyéndose un Proyecto Experimental bajo el nombre de "BolNet"[9], pionero de Internet en Bolivia generando servicios inicialmente de transmisión de datos comenzando por el Correo Electrónico (1990-1992) En el año 1991, se dieron los primeros pasos en la Internet, primero con una infraestructura alquilada y posteriormente en 1993, con la instalación de los equipos definitivos en la Facultad de Ingeniería Electrónica de la UMSA, logrando la comunicación 24 horas al día con 91 países. Se prestaba servicios a más de 1000 usuarios, incluyendo a instituciones académicas y científicas. La primera página web en Bolivia fue www.bolnet.b**o.** También dieron servicios como el acceso a base de datos,

[8] Microsoft ® Encarta ® 2008. © 1993-2007 Microsoft Corporation. Reservados todos los derechos.
[9] Red Troncal, para redes Científicas Acceso a Internet II y Gobierno en Línea

listas electrónicas, gopher y otros (1992-1995), los que desaparecieron con el advenimiento de los servicios full Internet y el servicio web[10].

En 1991 se asignó el código de país Internet para Bolivia " bo", pero fue recién en julio de 1995 que comenzaron a conectarse a Internet anfitriones con el nombre de dominio .bo. Dicha conexión fue posible gracias a un proyecto entre BolNet (unidad especial del Consejo Nacional de Ciencia y Tecnología (CONACYT), Red HUCYT (Red Hemisférica e Interuniversitaria sobre Ciencia y Tecnología) y el Programa de Desarrollo de las Naciones Unidas (PNUD)

ENTEL y BolNet, suscriben una alianza estratégica para la creación de Sistemas de Información y servicios (1996-1999), es así que BolNet coopera en la creación, desarrollo y expansión de la red ENTELNET conectando a las cuatro ciudades más importantes del país (La Paz, Santa Cruz, Cochabamba y Sucre) no sólo en ingeniería de redes, sino en el desarrollo de sistemas de administración y gestión de redes.

Concluido el convenio entre ENTEL S.A. y BolNet en diciembre de 1999, el Consejo Nacional de Ciencia y Tecnología, la Vicepresidencia de la República y el Ministerio de Educación, Cultura y Deportes, aprueban el nuevo Plan Estratégico de Bolnet para construir un Backbone Nacional para el Área Científica y Educativa y cooperación gubernamental.

Hasta mayo de 2000, se habían registrado 16 proveedores VAS[11] en SITTEL, de los cuales 12 eran proveedores de servicios relacionados a Internet, pero esta lista no era fija, debido a que no todos los operadores ISP del país se habían registrado, y sólo 10 ISP estaban en pleno funcionamiento.

---

[10] Bolivia en la Internet, 2da. Edición, pág. 18

[11] Servicio de valor añadido

Antes de la apertura de telecomunicaciones el único ISP que prestó servicio de Internet a 8 departamentos es ENTEL, el número de internautas a principios del año 2000 era de unos 90.000 hallándose el mayor número de usuarios de Internet en Santa Cruz, seguramente por el costo telefónico.

Cabe resaltar las palabras del entonces Vicepresidente de la República Ing. Jorge Quiroga R. "La incorporación y uso masivo de la Internet en la República permitirá otorgar mayor accesibilidad y rapidez a la información a un menor costo, aspirando a salvar las brechas de comunicación y tecnología que aun separan a grandes sectores de la sociedad boliviana, acción tendiente a facilitar sus demandas inmediatas de información".

Hoy en día en el Estado Plurinacional que dice ser netamente inclusivo es decir, incluir en todo ámbito a los sectores que antes estaban olvidados y que ahora son la gran mayoría, está realizando importantes esfuerzos en procura de modernizar al aparato gubernamental para poder ofrecer servicios en línea al ciudadano, a través del uso de las TIC´s[12]. (Tecnologías de Información y Comunicación).

La construcción de la Agenda Digital Boliviana, contribuirá para dotar al país de un horizonte y una estrategia estatal que permitan sentar las bases para dar un salto cualitativo de la sociedad hacia la Sociedad de la Información.

La actualización de la normativa en telecomunicaciones orientada a las TIC´s, permitirá crear un escenario moderno que garantice el uso y acceso eficiente de los recursos digitales, proteja al ciudadano y promueva la modernización.

[12] Comprende al conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento, transmisión y recepción de información, voz, datos, texto, video e imágenes. Se consideran como sus componentes el hardware, el software y los servicios.

El satélite Túpac Katari permitirá ofrecer conexión de Internet y servicios de telefonía de tipo satelital a poblaciones alejadas.

Con la vigencia de la reciente Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación del 08 de Agosto de 2011 que entre otras cosas promueve el uso de las tecnologías de información y comunicación para mejorar las condiciones de vida de las bolivianas y bolivianos y además Garantiza el desarrollo y la convergencia de redes de telecomunicaciones y tecnologías de información y comunicación, es decir que el Estado mediante políticas estratégicas está orientado a asegurar una conexión en cuanto a informática en todos los rincones de nuestro país.

1.4. ANTECEDENTES HISTORICOS DE DELITOS INFORMATICOS EN BOLIVIA

Los alcances de los delitos informáticos, llegan también a expresarse en Bolivia durante los últimos años.

En la gestión 1997 con la incorporación, en el Código Penal, con la tipificación de los delitos informáticos, se denuncian e investigan dos casos en la ciudad de La Paz, denuncias registradas en abril y octubre de 1997.

Durante el año 1998 no se registra ninguna denuncia significando para los análisis estadísticos de la PTJ (felcc actualmente) un decremento de -2 casos durante ese año.

El año 1999, nuevamente se verifican denuncias sobre manipulación informática en los departamentos de La Paz 1 caso, en Santa Cruz 2 y en Oruro 1, estableciéndose un incremento de +4 durante está gestión.

A inicios del año 2000, se manifiesta un verdadero incremento en este tipo de delitos llegando se a denunciar 13 casos en el ámbito nacional, 2 en la ciudad de La Paz, 2 en Cochabamba y 9 en Santa Cruz.

A inicios del siglo XXI con la significativa llegada de la tecnología al país se desato una serie de denuncias sobre delitos informáticos así como lo expresan los datos de la Fuerza Especial de Lucha Contra el Crimen (FELCC) revelando que en Santa Cruz, La Paz y Cochabamba se producen más delitos informáticos desde 2003, desde ese año hasta 2007, la Policía registró un total de 185 fraudes informáticos en todo el país, de éstos, 177 corresponden a manipulación informática y 8 a alteración, acceso y uso indebido de información. De la primera figura legal, 91 casos hubo en Santa Cruz, 46 en Cochabamba, 30 en La Paz, 4 en Potosí, 3 en Oruro, 2 en Beni y 1 en Tarija. Sobre alteración informática, 3 ocurrieron en La Paz, 2 en Cochabamba, 2 en Beni y 1 en Santa Cruz.

Entre enero y septiembre del año 2010, la Fuerza Especial de Lucha Contra el Crimen (FELCC) recibió al menos 50 denuncias de delitos informáticos en Bolivia, de las que sólo 36 están siendo investigadas, pero ninguna fue resuelta, por su complejidad y porque sólo hay un perito para atender ese tipo de casos. A ello se suma la falta de fiscales y policías investigadores especializados en esa materia para conducir las indagaciones.

La regulación de los delitos informáticos en Bolivia tipifica algunas de las formas importantes del fraude informático, pero es insuficiente para establecer agravantes de culpabilidad por nivel de conocimiento en materia informática.

Los delitos informáticos no contemplan además elementos de la ocultación dentro el fraude informático tales como la falsificación de realidades económicas, físicas o personales mediante uso de instrumentos informáticos.

1.5. HISTORIA DE LEGISLACION PENAL CONTRA DELITOS INFORMATICOS EN BOLIVIA

En Bolivia, el año 1997, se incluye dentro las reformas del Código Penal, en su Libro Segundo Título Xll, capítulo Xl, los artículos 363 bis y 363 ter, tipificaciones penales, que buscan regular la manipulación informática y la alteración, acceso y uso indebido de datos informáticos.

Podemos mencionar también que como parte de este esfuerzo regulador, el Poder Legislativo sanciona en 1992 la ley No. 1322 de derechos de autor y el Poder Ejecutivo dicta el Decreto Supremo No. 24582, del 25 de abril de 1997, denominado Reglamento de Soporte Lógico o Software, que velan por la protección de los derechos autorales en software y conforman una importante base para la formación de nuevas legislaciones en materia de derecho informático.

Las legislaciones penales bolivianas, de la década de los años 90 del siglo pasado, son una muestra de la necesidad de regulación específica de las acciones, derivadas del uso de la informática, en las relaciones comerciales.

Dentro del ordenamiento jurídico vigente, aún falta mucho que implementar legislativamente, para participar con el mundo y la región latinoamericana, en las operaciones que se desenvuelven en materia informática.

CAPITULO II

MARCO TEORICO
FUNDAMENTOS JURIDICOS DOCTRINALES SOBRE FALTA DE TIPICIDAD DEL FRAUDE INFORMATICO EN EL CODIGO PENAL BOLIVIANO

2.1. DERECHO INFORMÁTICO

El Derecho Informático, ha sido analizado desde diversas perspectivas, por un lado el Derecho Informático se define como: “Un conjunto de principios y normas que regulan los efectos jurídicos nacidos de la interrelación entre el Derecho y la informática.

Por otro lado hay definiciones que establecen que, “Es una rama del derecho especializado en el tema de la informática, sus usos, sus aplicaciones y sus implicaciones legales”.

El término "Derecho Informático" (Rechtsinformatik) fue acuñado por el Prof. Dr. Wilhelm Steinmüller[13], académico de la Universidad de Regensburg de Alemania, en los años 1970. Sin embargo, no es un término unívoco, pues también se han buscado una serie de términos para el Derecho Informático como Derecho Telemático, Derecho de las Nuevas Tecnologías, Derecho de la Sociedad de la Información, Ius cibernética, Derecho Tecnológico, Derecho del Ciberespacio, Derecho de Internet, etc.

[13] En www.vlex.com

Se considera que el Derecho Informático es un punto de inflexión del Derecho, puesto que todas las áreas del derecho se han visto afectadas por la aparición de la denominada Sociedad de la Información, cambiando de este modo los procesos sociales y, por tanto, los procesos políticos y jurídicos.

2.1.1. CONCEPTOS Y DEFINICIONES DE DERECHO INFORMATICO

La actividad informática en sus diversos aspectos, es en un principio regulada por un conjunto de normas de diferente contenido y asimismo, se caracteriza por un conjunto de principios e instituciones propias, por esta razón es pues importante dar un concepto de lo que se entiende por Derecho Informático y que nos permita ubicar con mayor claridad el objeto y la problemática de nuestro estudio, pasando a realizar un análisis de las diferentes definiciones de algunos autores:

- Para López Carrasco, el Derecho Informático “es el conjunto de normas que regulan las acciones, procesos, productos, y relaciones jurídicas surgidas en torno a la informática y sus aplicaciones”.

- Para Julio Téllez, el Derecho Informático “es el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la informática”.

- Para Emilio Suñe, el Derecho Informático “es el conjunto de normas reguladoras del objeto informático o de problemas directamente relacionados con la misma”.

- Para Juan José Ríos, el Derecho Informático “es el conjunto de normas jurídicas que regulan la creación, desarrollo, uso y aplicación

de la informática a los problemas que se deriven de la misma, en las que exista algún bien que deba ser tutelado jurídicamente por las propias normas".

2.2. LA INFORMATICA Y EL DERECHO

Una gran mayoría de estudiosos de la materia han señalado que el derecho informático "es el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad informática".

Al analizar las diferentes definiciones del derecho informático se tendrá también que analizar en profundidad la propia necesidad de incorporar el concepto de sistema como principio fundamental de la contratación informática, la aceptación de garantías y de las características propias de la responsabilidad civil y penal, que nos permitan identificar la existencia de este conjunto de principios e instituciones propias que caracterizan no solo al objeto sino, al conjunto de la estructura del derecho informático y sus regulaciones jurídicas por la urgente necesidad en las múltiples aplicaciones de la informática en el ámbito del derecho.

2.2.1. LA INFORMATICA JURIDICA

Con la aparición de la informática como la disciplina y el instrumento capaz de ordenar, clasificar, almacenar y procesar la información, el desarrollo de las ciencias y de la informática misma fue convirtiéndose en una carrera por alcanzar mayores funciones, mejor uso y desarrollo en esta técnica, tal es así que, debido a la necesidad doctrinal, a la jurisprudencia decisiónal y gestionaría, el derecho se convierte en el objeto de la informática[14], para ser

[14] En http://control.net/consultoría-inet.htm

tratada a través de esta para el mejor uso de los documentos, clasificación y archivo de su emisión normativa, permitiendo optimizar la labor del abogado y del juez como en las demás disciplinas, en el derecho son ya suficientes las bibliografías, los ficheros y los microfilmes para el manejo de la información, generándose una crisis con la aparición de la informática en la cual se ve una manera de solución a estos problemas con el tratamiento electrónico de estos datos jurídicos a través de la informática jurídica, es así que la computadora, con su gran capacidad de almacenamiento de datos y su portentosa velocidad de clasificación de las informaciones a través de innumerables canales de búsqueda y recuperación, logra concentrar mucha información y a mayor alcance de todos los juristas.

2.3. CONCEPTO DE DELITO

Para empezar a hablar de delitos informáticos es necesario primero señalar que entendemos por el término "delito".

El Código Penal de 1834 definía al delito en su Art. 1 señalando que "comete delito el que libre y voluntariamente y con malicia, hace u omite lo que la ley prohíbe o manda bajo alguna pena. En toda infracción libre de la ley se entenderá haber voluntad y malicia mientras que el infractor no pruebe, o no resulte claramente lo contrario"[15], en cambio el Código Penal en vigencia no da una definición de delito sino que en su parte especial enuncia los tipos especiales.

Para llegar a la definición que hoy conocemos de delito, tuvo que recorrer un largo camino, al ser un concepto dinámico que puede variar según la evolución

---

[15] Dr. Miguel Harb, Benjamín, Derecho Penal I, 4ta. Edición, 1992, Pág. 168

a la que esté sujeta la sociedad, es así que Ernest Beling[16] citado por Nodier Agudelo definía al delito como "la acción típica, antijurídica, culpable, sometida a una sanción penal adecuada, y conforme a las condiciones objetivas de punibilidad". Pero esta evolución dio paso a que se perfilen tres diversos conceptos según la diversa manera como se concebían cada uno de los elementos enunciados. Así de manera progresiva, fueron apareciendo el esquema Clásico, el Neoclásico y el Finalista.

Etimológicamente la palabra delito proviene del latín "delictum", expresión de un hecho antijurídico y doloso castigado con una pena. Existen características comunes y diferentes en cuanto a los tipos delictivos. El delito posee fundamentalmente tres elementos, la tipicidad, la antijuricidad y la culpabilidad.[17] Los mismos que serán brevemente explicadas:

> **a) La tipicidad,** originada por el penalista alemán Beling, para referirse a un elemento genérico del delito, es decir el tipo constituye la adecuación de la conducta a la figura descrita por la ley, al describir, el tipo no señala todas las circunstancias que concurren en la comisión del delito, sino que indica los elementos generales, por ello no es más que un esquema ideal o rector que sintetiza las notas constitutivas del delito[18] debiendo esta acción estar prevista en la ley para que pueda castigarse. Distinguiéndose en la tipicidad un aspecto objetivo referido a los elementos descriptivos y normativos; y un aspecto subjetivo caracterizado por la concurrencia del dolo o la culpa y determinados elementos subjetivos adicionales, de acuerdo con lo expuesto por el Dr. Benjamín M. Harb el tipo cumple principalmente dos funciones: Una de

[16] Nódier Agudelo Betancur, Curso de derecho Penal, Ediciones Nuevo Foro, 1998, Pág. 20-21
[17] Ob. Cit. Pág. 161

[18] Ob. Cit. Pág. 218

garantía porque limita el Ius puniendi sólo a los actos definidos por el tipo y la otra función es constituir la base del delito.

b) La antijuricidad, conocida por la doctrina española como "injusto", constituyéndose el elemento valorativo del delito, a través del cual se afirma que la acción debe oponerse al ordenamiento jurídico y no justificarse, debiendo lesionar o poner en peligro un interés jurídicamente protegido, si concurriere alguna causal de justificación, la conducta típica no será antijurídica y, por lo tanto, no constituirá delito.

c) La culpabilidad, conocida como la responsabilidad criminal del autor del hecho delictuoso, Benjamín Miguel Harb indica que la culpabilidad es la situación en la que se encuentra un individuo imputable y responsable a quien el juez declara merecedor de una pena[19].

Las características comunes a todo delito son: la tipicidad, la antijuricidad y la culpabilidad, ya que si no existiera la tipicidad, no habrían las bases para determinar la antijuricidad y la culpabilidad, por tanto, si concurren todos estos elementos hay delito. Ante la falta de uno de estos requisitos, no habría la comisión de un delito.

2.4. ASPECTOS GENERALES DE DELITOS INFORMATICOS

El progreso tecnológico cada día es más importante y sostenido de los sistemas computacionales permite hoy procesar y poner a disposición de la sociedad una cantidad creciente de información de toda naturaleza, al alcance concreto de millones de interesados y de usuarios. Las más diversas esferas del

[19] En http://www.monografias.com

conocimiento humano, en lo científico, en lo técnico, en lo profesional y en lo personal están siendo incorporadas a sistemas informáticos que, en la práctica cotidiana, de hecho sin limitaciones, entrega con facilidad a quien lo desee un conjunto de datos que hasta hace unos años sólo podían ubicarse luego de largas búsquedas y selecciones en que el hombre jugaba un papel determinante y las máquinas existentes tenían el rango de equipos auxiliares para imprimir los resultados. En la actualidad, en cambio, ese enorme caudal de conocimiento puede obtenerse, además, en segundos o minutos, transmitirse incluso documentalmente y llegar al receptor mediante sistemas sencillos de operación, confiables y capaces de responder casi toda la gama de interrogantes que se planteen a los archivos informáticos.

Puede sostenerse que hoy las perspectivas de la informática no tienen límites previsibles y que aumentan en forma que aún puede impresionar a muchos actores del proceso.

Este es el panorama de este nuevo fenómeno científico tecnológico en las sociedades modernas. Por ello ha llegado a sostenerse que la Informática es hoy una forma de Poder Social. Las facultades que el fenómeno pone a disposición de Gobiernos y de particulares, con rapidez y ahorro consiguiente de tiempo y energía, configuran un cuadro de realidades de aplicación y de posibilidades de juegos lícitos e ilícitos, en donde es necesario el derecho para regular los múltiples efectos de una situación, nueva y de tantas potencialidades en el medio social.

Esta marcha de las aplicaciones de la informática no sólo tiene un lado ventajoso sino que plantea también problemas de significativa importancia para el funcionamiento y la seguridad de los sistemas informáticos en los negocios, la administración, la defensa y la sociedad.

Debido a esta vinculación, el aumento del nivel de los delitos relacionados con los sistemas informáticos registrados en la última década en los Estados Unidos, Europa Occidental, Australia y Japón, representa una amenaza para la economía de un país y también para la sociedad en su conjunto.

De acuerdo con la definición elaborada por un grupo de expertos, invitados por la OCDE a París en mayo de 1983, el término delitos relacionados con las computadoras se define como cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos. La amplitud de este concepto es ventajosa, puesto que permite el uso de las mismas hipótesis de trabajo para toda clase de estudios penales, criminológicos, económicos, preventivos o legales.

En la actualidad la informatización se ha implantado en casi todos los países, tanto en la organización y administración de empresas y administraciones públicas como en la investigación científica, en la producción industrial o en el estudio e incluso en el ocio, el uso de la informática es en ocasiones indispensable y hasta conveniente. Sin embargo, junto a las incuestionables ventajas que presenta comienzan a surgir algunas facetas negativas, como por ejemplo, lo que ya se conoce como "criminalidad informática".

El espectacular desarrollo de la tecnología informática ha abierto las puertas a nuevas posibilidades de delincuencia antes impensables. La manipulación fraudulenta de los ordenadores con ánimo de lucro, la destrucción de programas o datos y el acceso y la utilización indebida de la información que puede afectar la esfera de la privacidad, son algunos de los procedimientos relacionados con el procesamiento electrónico de datos mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños materiales o morales. Pero no sólo la cuantía de los perjuicios así ocasionados es a menudo infinitamente superior a la que es usual en la delincuencia tradicional, sino que también son mucho más elevadas las posibilidades de que

no lleguen a descubrirse. Se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La informática reúne unas características que la convierten en un medio idóneo para la comisión de muy distintas modalidades delictivas, en especial de carácter patrimonial (estafas, apropiaciones indebidas, etc.). La idoneidad proviene, básicamente, de la gran cantidad de datos que se acumulan, con la consiguiente facilidad de acceso a ellos y la relativamente fácil manipulación de esos datos.

La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, los ha transformado en un objeto cuyo ataque provoca un perjuicio enorme, que va mucho más allá del valor material de los objetos destruidos[20]. A ello se une que estos ataques son relativamente fáciles de realizar, con resultados altamente satisfactorios y al mismo tiempo procuran a los autores una probabilidad bastante alta de alcanzar los objetivos sin ser descubiertos.

2.4.1. CONCEPTOS Y DEFINICIONES DEL DELITO INFORMÁTICO

El autor mexicano Julio Téllez Valdez señala que los delitos informáticos son "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin (concepto atípico) o las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin (concepto típico)". Por su parte, el tratadista penal italiano Carlos Sarzana, sostiene que los delitos informáticos son "cualquier comportamiento criminal en que la computadora está involucrada como material, objeto o mero símbolo".

[20] En http://www.htcn.org

Debemos considerar que el nacimiento de este delito se encuentra íntimamente asociado al desarrollo tecnológico informático[21] y el hecho de definir y delimitar el delito informático es una labor ardua, considerándose a nivel internacional que no existe una definición propia del *delito informático*, dado su carácter especial, por lo tanto no debemos tipificar todas las conductas donde interviene un elemento del ámbito de la informática como un delito informático. De mantenerse esta postura acabaría por considerarse a cualquier conducta delictiva en la que se vea implicado un sistema informático como delito informático.[22]

Por otra parte, se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se utiliza un computador o un sistema informático, tales como ***"delitos informáticos", "delitos electrónicos", "delitos relacionados con las computadoras", "crímenes por computadora", "delincuencia relacionada con el ordenador"***, etc.[23] siendo la más adecuada el termino **Delito Informático** en sentido de las ventajas que ofrece, en este sentido Romeo Casabona[24] indica que el término Delito Informático debe usarse en su forma plural, en atención a que se utiliza para designar una multiplicidad de conductas ilícitas y no una sola de carácter general, así tenemos las siguientes definiciones y conceptos:

- Para Carlos Sarzana[25], en su obra Criminalística y Tecnología, los crímenes por computadora comprenden cualquier comportamiento

[21] Huerta M. Marcelo.-Claudio Líbano M, Delitos informáticos; Editorial jurídica Cono Sur Ltda., 1996, Pág. 106.

[22] En el desarrollo de la investigación se encontró la sugerencia de tipificar como homicidio "informático" el caso del médico que prescribe una medicina mediante correo electrónico a un paciente y le altera la receta, siendo claro el Art. 251 el que matare a otro será sancionado con presidio de 5 a 20 años, a mi parecer no podemos incurrir en ese error de catalogar todo accionar en el que medie un sistema informático como "delito informático".

[23] En www.delitosinformaticos.com

[24] Citado por Huerta-Líbano, Delitos Informáticos, Pág. 111

[25] En http:publicaciones.derecho.org

criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo.

- Ma. Cinta Castillo J. y Miguel Ramallo R[26]., es toda acción dolosa que provoca un perjuicio a personas o entidades en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas.

- Para Marcelo Huerta M. y Claudio Líbano M.[27], son todas aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual, generalmente, producirá de manera colateral lesiones a distintos valores jurídicos, reportándose, muchas veces un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro.

- Nidia Callegari[28], define al delito informático como aquel que se da con la ayuda de la informática o de técnicas anexas.

- Ulrich Sieber[29], señala que el delito informático comprende todas las lesiones dolosas e ilícitas del patrimonio relacionadas con datos procesados automáticamente.

---

[26] Ob.cit.Pag.114
[27] Ob. Cit. Pág. 116

[28] En http://publicaciones.derecho.org
[29] Ibíd.

- Rafael Fernández Calvo[30], define al delito informático 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 o telemático contra los derechos y libertades de los ciudadanos definidos en el Título I de la Constitución Española.

- National Center for Computer Crime Data[31], incluye todos los delitos perpetrados por medio del uso de computadores y todos los delitos en que se dañe a los computadores o a sus componentes.

- María de la Luz Lima[32], dice que el delito electrónico en un sentido amplio, es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin, y en un sentido estricto, el delito informático es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin.

- La Organización para la Cooperación Económica del Desarrollo (OCDE) ha definido al delito informático como cualquier conducta ilegal, no ética, o no autorizada que involucra el procesamiento de datos y/o la transmisión de datos.

- Jijena Leiva[33], define a los delitos informáticos como toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma.

---

[30] Ibíd.
[31] Ob. Cit. Pág. 114
[32] En http://publicaciones.derecho.org
[33] Ibíd.

- Tiedemann[34], define al delito informático como aquel acto antijurídico que para su comisión se emplea un sistema automático de procesamiento de datos o de transmisión de datos.

- Julio Téllez Valdez[35], 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, este tipo de acciones presentan las siguientes características principales :

  a) Son conductas criminales de cuello blanco (White collar crime), en tanto que sólo un determinado número de personas con ciertos conocimientos (en este caso técnicos y profesionales) pueden llegar a cometerlas.

  b) Son acciones ocupacionales, en cuanto a que muchas veces se realizan cuando el sujeto se halla trabajando.

  c) Son acciones de oportunidad, ya que se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.

  d) Provocan serias pérdidas económicas, ya que casi siempre producen "beneficios" de más de cinco cifras a aquellos que las realizan.

---

[34] Ibíd.
[35] En http://publicaciones.derecho.org

e) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia fisica pueden llegar a consumarse.

f) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.

g) Son muy sofisticados y relativamente frecuentes en el ámbito militar.

h) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.

i) Ofrecen facilidades para su comisión a los menores de edad.

j) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.

k) Por el momento siguen siendo ilícitos impunes de manera manifiesta ante la ley.

La mayoría de los autores citados coinciden al dar el concepto de delito informático en el medio comisivo siendo un sistema informático o base de datos, Sin embargo para *Davara Rodriguez*[36] no parece adecuado hablar de delito informático ya que, como tal, no existe, si atendemos a la necesidad de una tipificación en la legislación penal para que pueda existir un delito.

[36] Sin embargo, distingue dentro de la manipulación mediante la informática des vertientes: a) Acceso y manipulación de datos y b) manipulación de los programas. En http://publicaciones.derecho.org/redi/No._06_-_Enero_de_1999/cuervo

Partiendo de que los Programas de informática pueden ser vulnerados y los de sistemas de seguridad basados en el software son vulnerables, analizados los conceptos anteriormente señalados, para la presente tesis entenderemos por delitos informáticos "**cualquier conducta ilícita susceptible de ser sancionada, utilizando la tecnología informática para su comisión".**

La delincuencia informática es un conjunto de comportamientos dignos de reproche penal que tienen por instrumento o por objeto a los sistemas o elementos de técnica informática, o que están en relación significativa con ésta pudiendo presentar múltiples formas de lesión de variados bienes jurídicos.[37]

Para no caer en el error de configurar a todas las conductas antisociales que tengan como medio de comisión un sistema informático y enmarcarlas como delitos informáticos, es necesario determinar el objeto de protección al que se pretende otorgar protección penal, lo cual brindará los índices necesarios o no de un delito informático con autonomía.

2.4.2. BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS

El Dr. Benjamín M. Harb señala según el derecho, bien es todo lo que tiene significación jurídica o como dice Ihering, lo que es útil, lo que es apto para satisfacer las necesidades humanas. Puede consistir en objetos físicos o cualidades, etc.[38] Entonces un bien con carácter social deberá ser amparado a través de los órganos legisladores, constituyéndose en el punto de referencia para la determinación de la tipificación de una conducta que se considere delictiva.

---

[37] Ver en http://publicaciones.derecho.org/redi/No._06_-_Enero_de_2009/cuervo

[38] Ob. Cit. Pág. 201

Una de las corrientes que se ha generado en torno a la discusión de los bienes jurídicos en los delitos informáticos, es aquella posición en la que se adecua o amplia el tipo penal clásico con los hechos informáticos, tal es el caso de Argentina, cabe mencionar que esta posición acarrea la dificultad como por ejemplo en el tipo penal de la estafa el engaño o ardid a una máquina, lo contrario con Estados Unidos que tienen la posición de crear tipos penales informáticos.

Las diferentes conductas nocivas que se cometen a través de sistemas informáticos y en Internet pueden ocasionar diversas lesiones a diferentes bienes jurídicos protegidos, tales como la intimidad, el patrimonio y nuevos objetos jurídicos de protección que adquieren autonomía e identidad propias en la red, a continuación analizaremos tales bienes jurídicos.

2.4.2.1. LA INTIMIDAD COMO BIEN JURÍDICO PROTEGIDO

El derecho a la intimidad tuvo su primera expresión en el "right tobe let alone" (Derecho a ser dejado solo) del derecho anglosajón, el que posteriormente ha recibido la denominación de derecho a la intimidad o a la privacidad. Muchos autores no hacen diferencia alguna respecto a los términos intimidad y privacidad, más bien lo toman como sinónimos.

El diccionario de la Real Academia define la intimidad como "la zona espiritual íntima y reservada de una persona o un grupo, especialmente de una familia". Cabanellas señala que intimidad es una parte personalísima y reservada de un caso o persona. Su revelación puede originar responsabilidad cuando cause perjuicio y haya dolo o grave imprudencia; pero, si se trata de actividad preliminar del delito, entonces la denuncia resulta a veces un deber; según Herrán Ortiz "por el vocablo intimidad se alude tanto al carácter oculto o secreto

de aquellas circunstancias que rodean la existencia de un individuo, como a las circunstancias internas, esenciales del hombre y que éste mantiene como núcleo de su personalidad”.

Muñoz Conde señala que el “derecho a la intimidad trata de tutelar la voluntad de una persona física o jurídica de que no sean conocidos determinados hechos que tan sólo ella o un número limitado de personas conoce".

Ferreira Rubio Delia determina que la privacidad es un término general que da a entender todo lo concerniente a una persona y que no debe estar en conocimiento de los demás. En cambio intimidad es un término más específico nos da a entender todo lo concerniente a lo más profundo del ser humano, a aquellos aspectos que solo son reservados para esa persona, su conciencia e inherente a su propia personalidad.

En el plano internacional, el derecho a la intimidad es reconocido por la Declaración Universal de Derechos Humanos de las Naciones unidas de 1948 en su Art. l2, la Convención Europea para la protección de los Derechos Humanos y de las Libertades Fundamentales de 1950 en su Art. 8.1, y en el Art. 17.1 del Pacto Internacional de Derechos Civiles y Políticos de 1966.

Con la denominada sociedad de la información el individuo se ha visto más vulnerable en cuanto a su intimidad, hasta el punto de solicitar instrumentos jurídicos adecuados para preservar su derecho, al ser latente tal violación a través de Internet, por la facilidad que otorgan los computadores en el acopio, tratamiento, transmisión y almacenamiento de información, el hecho de que los datos registrados pueden utilizarse fraudulentamente e ir a parar en manos de personas no autorizadas; es así que en Alemania se han establecido leyes que establecen el manejo de los datos de carácter personal por parte de las autoridades y los particulares, en 1990 se actualizo la Ley Federal para el

Desarrollo de Elaboración y Protección de datos, modificada por la ley sobre el Nuevo Ordenamiento de Sistema de correo y de las Telecomunicaciones de 1994, estableciéndose que todo ciudadano tiene derecho a recibir la información sobre los datos almacenados en relación con su persona, pudiendo exigir la corrección de datos falsos, el bloqueo de datos litigiosos y la cancelación de datos recopilados ilícitamente, siendo uno de los países que posee una legislación moderna y completa en relación a la protección de datos, al contar con el Delegado federal para la protección de datos cuya función consiste en asesorar al Gobierno y al Parlamento en los procedimientos legislativos desde la óptica de la protección de los datos personales, controlar el manejo de los datos personales por parte de las autoridades de la Federación y presentar recomendaciones en orden al mejoramiento de la protección de dichos datos. Todo ciudadano que considere lesionados sus intereses en este campo por una autoridad de la Federación puede someter su caso al Delegado. Asimismo las empresas dedicadas al procesamiento de datos están obligadas a designar un comisionado para la protección de datos.

En España a través de la Ley Orgánica 5/92 de Regulación del Tratamiento Automatizado de Datos de Carácter Personal (LORTAD) modificada por la Ley Orgánica 15/99 "Ley de Protección de Datos de Carácter Personal” (LOPD), se establecen los siguientes principios, principio de calidad de los datos personales, que prevé que sólo podrán recogerse datos de carácter personal para su tratamiento automatizado, cuando tales datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades legítimas para las que se haya obtenido; el principio de la transparencia y publicidad del tratamiento, vinculado a brindar informaciones precisas a los interesados para que puedan contrastar y evaluar la incidencia y alcance que en sus derechos y libertades fundamentales va a tener el tratamiento automatizado de sus datos personales; el principio de seguridad de los datos de carácter personal, que establece la obligación del responsable del fichero de adoptar las medidas de

índole técnica y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, perdida, tratamiento o acceso no autorizado; el principio del consentimiento, que exige que en todo tratamiento automatizado de datos de carácter personal se deberá requerir la autorización del afectado.

Si bien el Art. l8 del Código Civil toma en cuenta el derecho a la intimidad como un derecho de la personalidad, nuestro Código Penal no toma como tipo penal la violación al derecho de la intimidad, como es el caso del Perú que establece una pena no mayor a dos años cuando se viola la intimidad personal o familiar sea mediante procesos técnicos u otros medios, con el empleo del término **"u otros medios"** deja a la interpretación el uso de nuevas tecnologías.

2.4.2.2. EL PATRIMONIO COMO BIEN JURÍDICO PROTEGIDO

El patrimonio está constituido por la suma de los valores económicos puestos a disposición de una persona, bajo la protección del ordenamiento jurídico.

Con el desarrollo del comercio electrónico, la informatización de las transacciones financieras, comerciales y bancarias, la generalización del pago a través de procedimientos electrónicos, ha abierto nuevas posibilidades de atentar contra el patrimonio, convirtiéndose como uno de los principales bienes jurídicos objetos de protección en la red, toda vez que la amplia gama de fraudes a través de manipulaciones informáticas atentan contra dicho bien jurídico.

2.4.2.3. EL HONOR COMO BIEN JURÍDICO PROTEGIDO

El derecho al honor constituye el derecho que cada ser humano tiene al reconocimiento y respeto ante él mismo y ante las demás personas, de su

dignidad humana y de los méritos y cualidades que ha ido adquiriendo como fruto de su desarrollo personal y social.

Si bien existe una cercanía entre intimidad y honor, ambos representan diferentes bienes protegidos, ya que el primero se caracteriza por el derecho del individuo a preservar su vida privada de cualquier injerencia ajena, mientras que el segundo se define por el derecho al respeto que merece toda persona en su dignidad humana.

El uso del Internet puede ser el medio para afectar el derecho al honor como por ejemplo el envío de publicaciones en páginas web con información que atente el honor de determinadas personas, siendo la diferencia con el tipo clásico el empleo de sistemas informáticos por lo tanto no configura un delito informático en la medida que el medio empleado representa sólo una característica de la conducta.

Nuestro Código Penal en lo referente a los delitos contra el honor toma en cuenta a la persona jurídica como sujeto pasivo en su Art. 282 (Difamación) implícitamente en el Art. 287 (Injuria), más no en el delito de calumnia (Art.283), recogiendo de esta manera la concepción de que las personas jurídicas tienen derecho al honor.

Por tanto, el honor se considera como bien protegido en los delitos informáticos, ya que si se introducen publicaciones que afecten la reputación, honra y personalidad de una persona en medios informáticos y tomando en cuenta que estos medios superan fronteras, puede acarrear una muerte civil de la misma.

2.5. LA TEORIA ESTRUCTURALISTA Y EL DERECHO

La línea a la cual sigue la presente investigación es a la escuela Sociológica el cual una de los pioneros es Emile Durkheim (1858-1917), autor de tres obras claves de la moderna Sociología (Las reglas del método, El suicidio y De la división, parte de la observación de un dato sobre el que ya llamaron la atención los “estadísticos morales”: el volumen constante de la criminalidad; esto es, la existencia inevitable, en cualquier tipo de sociedad y en cualquier momento histórico, de una tasa constante de delincuencia. De tal hecho infirió Durkheim dos consecuencias: la conducta irregular es inextirpable, desde el momento en que la conducta social se concibe como conducta “reglada” (regulada por normas); y las formas de dicha conducta “anómica” estarán determinadas, en cada caso, por el tipo social dominante y su estado de desarrollo. Frente a las concepciones tradicionales, la tesis de Durkheim significa, en definitiva, admitir que el delito es un comportamiento “normal” (no patológico), “ubicuo” (Se produce en cualquier estrato de la pirámide social, y en cualquier modelo de sociedad) y derivado no de anomalías del individuo ni de la propia “desorganización social”, sino de las estructuras y fenómenos cotidianos en el seno de un orden social intacto.

Una determinada cantidad de crímenes forma parte integrante de toda sociedad sana, y una sociedad sin conductas irregulares sería una sociedad poco desarrollada, monolítica, inmóvil y primitiva.

La propia “pena”, según el autor, no cumple los fines metafísicos que tradicionalmente se le asignan, sino que surge como cualquier otra institución social de las relaciones estructural-funcionales.

Asimismo Edwin Sutherland dice “el delito no es algo anormal, ni signo de una personalidad inmadura, sino un comportamiento o habito adquirido, una respuesta a situaciones reales que el sujeto aprende”.

El crimen se aprende de la misma forma que la conducta conformista por vía de los procesos comunicacionales y las relaciones interpersonales que se entablan.

Los mecanismos de aprendizaje de la conducta criminal no pueden limitarse al hecho de situarse en el contexto criminal, pues es fundamental y crucial importancia el hecho de la interacción del individuo como parte de ese proceso de aprendizaje.

En este sentido, para la teoría una persona se convierte en criminal cuando las definiciones favorables al crimen superan a las definiciones desfavorables. Su proceso de aprendizaje se diferencia por internalizar conductas de carácter criminal en mayor proporción que las conductas conformistas.

Es importante destacar que la teoría de la asociación diferencial de Sutherland ha sido observada como una corrección para explicar la criminalidad de las clases altas del estructuralismo. De allí, la importancia de los trabajos confeccionados respecto de esta criminalidad denominada “de cuello blanco”. Por criminalidad de cuello blanco entendemos a aquella que realizan personas de elevada posición social en ejercicio de un poder económico o político que les garantiza impunidad.

La libertad individual queda seriamente afectada, porque el hombre es un objeto de imputación de lenguaje, códigos, símbolos, pautas y valores criminales, que asimila sin consideración alguna de su parte.

Entonces llegamos a la conclusión de que no cualquier delincuente puede ser un delincuente informático, sino que este debe tener distintos aspectos que se mencionan líneas abajo.

2.5.1. SUJETOS DE LOS DELITOS INFORMÁTICOS

De acuerdo con el derecho penal en la ejecución de un delito supone la existencia de dos personas: Sujeto activo y sujeto pasivo, respecto a este punto el Dr. Benjamín Miguel[39] indica que el sujeto activo del delito es el hombre, puesto que por su naturaleza física visible y capacidad de hecho y de derecho posee responsabilidad, en cuánto al sujeto pasivo o víctima es el titular del bien jurídico lesionado sea una persona individual o jurídica, nuestra legislación adopta la postura de que sólo el hombre puede ser sujeto activo de un delito y no así una persona jurídica.

2.5.1.1. SUJETO ACTIVO

Los sujetos que cometen los denominados delitos informáticos poseen ciertas particularidades que los diferencian del común de los delincuentes, siendo sus características las siguientes:

- Son personas que no poseen antecedentes delictivos.
- La mayoría de sexo masculino, cuya edad oscila entre los 15 y los 30 años.
- Actúan en forma individual rara vez lo hacen en grupo.
- Son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico.
- Son jóvenes con gran solvencia en el manejo de la computadora, con coraje, temeridad y una gran confianza en sí mismo.

[39] Ob. Cit. Pág. 191-192

- También hay técnicos no universitarios, autodidactas, competitivos, con gran capacidad de concentración y perseverancia. No se tata de delincuentes profesionales típicos, y por eso, son socialmente aceptados.

- En el caso de los "hackers", realizan sus actividades como una especie de deporte de aventura donde el desafío esta allí y hay que vencerlo.

- Dentro de las organizaciones, las personas que cometen fraude han sido destacadas en su ámbito laboral como muy trabajadoras, muy motivadas (es el que siempre está de guardia, el primero en llegar y el último en irse).

Teniendo en cuenta las características del sujeto activo de los "delitos informáticos", estudiosos en la materia los han catalogado como *"delincuentes de cuello blanco"* término introducido por primera vez por el criminólogo norteamericano Edwin Sutherland en el año de 1943, quién señala un sin número de conductas que considera como "delitos de cuello blanco"' aún cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe destacar las "violaciones a las leyes de patentes y fábrica de derechos de autor, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios, entre otros". Asimismo, dice que tanto la definición de los "delitos informáticos" como la de los "delitos de cuello blanco" no son de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. La característica común que poseen ambos delitos tenemos que son personas de cierto status socioeconómico, es decir que en estos delitos técnicos, difícilmente podría considerarse como móviles que inducen al delincuente la poca preparación o la situación económica sino por el contrario es el reto y la facilidad en la obtención de los medios los elementos que enmarcan este tipo de delitos.

Asimismo el sujeto activo según su posición frente al sistema informático se clasifica en:

- **Sujetos Internos** que son personas que trabajan dentro de una empresa o institución que tienen un acceso autorizado al sistema, conociendo de las diferentes rutinas de trabajo, que tienen identificado el acceso, método y resultado, para la comisión de su pretensión y los
- **Sujetos Externos** que son aquellos individuos que utilizando sus conocimientos técnicos pueden acceder a la información, desde fuera del lugar del establecimiento.

2.5.1.1.1. EL HACKER[40]

En informática, un Hacker [41]es una persona con mucho conocimiento en este campo, capaz de descifrar códigos para ingresar a base de datos dentro de los soportes informáticos de instituciones públicas o privadas pero también a cuentas en la red como el correo electrónico "Facebook[42]" de personas particulares, El Hacker ingresa a un sitio en la red con el único propósito de aventura o la de un reto a sus propios conocimientos tratando de superar siempre sus limitaciones, generalmente son gente apasionada por la seguridad informática. Esto concierne principalmente a entradas remotas no autorizadas por medio de redes de comunicación como Internet.

[40] Los hackers son fruto de los cambios generados en la década de los años 60 y 70, buscan expresar "arte", en la red Internet, pero sus actividades suelen dañar los sistemas informáticos a nivel mundial. (RSPA.COM:2010).
[41] http://es.wikipedia.org/wiki/Hacker
[42] Red social, donde la gente interactúa comunicándose a larga distancia.

En la actualidad la palabra Hacker se usa de forma corriente para referirse mayormente a los criminales informáticos, debido a su utilización masiva por parte de los medios de comunicación desde la década de 1980.

2.5.1.1.2. EL CRACKER

El cracker, [43]es considerado un "vandálico virtual". (Analogía de "safecracker", que en español se traduce como "un ladrón de cajas fuertes"). Este utiliza sus conocimientos para invadir sistemas, descifrar claves y contraseñas de programas y algoritmos de encriptación, ya sea para poder correr juegos sin un CD-ROM, o generar una clave de registro falsa para un determinado programa, robar datos personales, o cometer otros ilícitos informáticos. Algunos intentan ganar dinero vendiendo la información robada, otros intentan embaucar o chantajear con la información obtenida. Es por ello que debemos ser extremadamente precavidos con el manejo de la información que tenemos almacenada en nuestra PC, y protegerla debidamente con algún buen sistema de seguridad.

Cracker es el término que define a programadores maliciosos y ciberpiratas que actúan con el objetivo de violar ilegal o inmoralmente sistemas cibernéticos, siendo un término creado en 1985 por los hackers en defensa del uso periodístico del término.

2.5.1.1.3. DIFERENCIAS ENTRE HACKER Y CRACKER

Planteados los conceptos de hacker y cracker podemos establecer unas cuantas diferencias entre éstos individuos:

---

[43] http://es.wikipedia.org/wiki/Cracker

Por lo general, [44]el término “hacker” suele utilizarse de manera errónea en la informática, a un hacker suelen asociarlo con las personas que realizan actos ilícitos por medio de las computadoras (phishing, virus, desfases, etc.), esta es una idea completamente errónea pues se podría decir que los hackers son los buenos (los que programan el software que utilizamos) y los crackers son los malos (aquellos que se encargan de vulnerar los software que crean los hackers).

La diferencia clave entre un hacker y un cracker es que el cracker vulnera el software el cual es un sistema que el hacker crea.

Por lo tanto, un hacker y un cracker son dos personas, si bien, con conocimientos similares, pero con ideas completamente diferentes. En los hackers suele existir un código de ética, contrario a los crackers que se valen de cualquier medio para lograr su objetivo.

2.5.1.2. SUJETO PASIVO

En primer término tenemos que distinguir que sujeto pasivo ó víctima del delito es el ente sobre el cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los "delitos informáticos" las víctimas pueden ser individuos, instituciones crediticias, gobiernos, etcétera que usan sistemas automatizados de información, generalmente conectados a otros, mediante él podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, con el objeto de prever las acciones antes mencionadas debido a que muchos de los delitos son descubiertos casuísticamente por el desconocimiento del modus operandi de los sujetos activos.

Las características del sujeto pasivo son las siguientes:

[44] http://culturacion.com/2009/05/hacker-y-cracker-%C2%BFcual-es-la-diferencia/

- El sujeto pasivo puede ser una persona particular, empresas, instituciones públicas, etc., que utilizan sistemas automatizados de información, generalmente conectados a otros.

- Síndrome de avestruz es decir temor de denunciar ante el desprestigio que pudiera ocasionarles y sus consecuentes pérdidas económicas.

2.6. CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS

Ponemos a continuación algunas clasificaciones que se dieron en relación a los delitos informáticos:

2.6.1. CLASIFICACIÓN SEGÚN JULIO TELLEZ VALDES[45]

Clasifica a los delitos informáticos en base a dos criterios: como instrumento o medio, o como fin u objetivo.

2.6.1.1. COMO INSTRUMENTO O MEDIO

Se tienen a las conductas criminógenas que se valen 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.

[45] En http://publicaciones.derecho.org

c) Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.)

d) Lectura, sustracción o copiado de información confidencial.

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

f) Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.

g) Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria ficticia.

h) Uso no autorizado de programas de cómputo.

i) Introducción de instrucciones que provocan "interrupciones" en la lógica interna de los Programas.

j) Alteración en el funcionamiento de los sistemas, a través de los virus[46] informáticos.

k) Obtención de información residual impresa en papel luego de la ejecución de trabajos.

[46] En 1984 el Dr. Fred Cohen clasificó a los virus en 2 categorfas:1. Trojan horses (caballos de Troya); 2. Worms: gusanos. Las clasificaciones de segunda generación dividieron a los virus en 3 categorías: a) VIRUS DE BOOT que infectan la memoria y atacan al sector de arranque de los disquetes y el disco duro y desde cuya posición pueden infectar a los archivos y áreas del sistema. b) VIRUS DE SISTEMA, producidos para afectar en primer lugar al COMMAND.COM y posteriormente a otras áreas vitales del sistema informático. c) VIRUS DE ARCHIVOS EJECUTABLES, aquellos con extensión COM y EXE. y a partir de 1995 se conocen los MACRO VIRUS variante que afecta archivos ejecutables sino archivos de documento. (PERSYSTEMS.COM:2001)

l) Acceso en áreas informatizadas de forma no autorizada.

m) Intervención en las líneas de comunicación de datos o teleproceso.

2.6.1.2. COMO FIN U OBJETIVO

En esta categoría se enmarcan las conductas criminógenas 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.

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

f) Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje. (pago de rescate, etc.).

2.6.2. CLASIFICACIÓN SEGÚN MARÍA DE LA LUZ LIMA[47]

Presenta una clasificación, de lo que ella llama *"delitos electrónicos",* a las categorías señaladas por Téllez Valdez agrega a los que la tecnología

[47] Ibíd.

electrónica utiliza como método (se utilizan métodos electrónicos para llegar a un resultado ilícito) diciendo que existen tres categorías, a saber:

a. Los que utilizan la tecnología electrónica como método,

b. Los que utilizan la tecnología electrónica como medio y

c. Los que utilizan la tecnología electrónica como fin.

a. Como método, son conductas criminógenas donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

b. Como medio, son conductas criminógenas donde para realizar un delito utilizan una computadora como medio o símbolo.

c. Como fin, son conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

2.6.3. CLASIFICACIÓN SEGÚN URLICH SIEBER[48]

Este autor alemán clasifica los delitos informáticos en los siguientes grupos:

a. Delitos de fraude mediante la manipulación de los datos.

b. Delitos de espionaje informático, piratería de software y sustracción de alta tecnología.

c. Delitos de sabotaje informático.

[48] Ob. Cit. Pág. 122

d. Delitos de sustracción de servicios.

e. Delitos de acceso indebido.

f. Delitos de fraude fiscal relacionados con el computador.

2.6.4. CLASIFICACIÓN DE MARCELO HUERTA Y CLAUDIO LIBANO[49]

Estos autores chilenos clasifican los delitos informáticos:

a. La manipulación indebida de datos a través de la utilización de un sistema de tratamiento de la información. El fraude informático.

b. Tal manipulación puede realizarse en la entrada de datos al sistema (input), en los programas, en la salida de datos del sistema (output).

c. Delitos de espionaje informático. Se incluyen las formas de acceso no autorizado a un sistema de tratamiento de la información.

d. Delitos de sabotaje informático. Incluyen las formas de destrucción y alteración de datos, así como los programas virus.

e. Delitos de piratería de programas. Sólo en cuando se traduzca en la copia indebida de programas por medios informáticos.

f. Delitos de hacking, en sus distintas manifestaciones que se analizaran más adelante.

[49] Ob. Cit. Pág. 123

CAPITULO III
MARCO TEORICO
EL FRAUDE INFORMATICO SUS ALCANCES Y COMPLICACIONES.

3.1. ASPECTOS GENERALES DE FRAUDE INFORMATICO

La palabra Fraude proviene del latín "fraudem" mala fe, entendiéndose que obrar en fraude es aquel que no hace lo que debe hacer, el escritor Juan Rodríguez[50] sitúa el primer gran fraude cometido en la historia de la humanidad en base a datos bíblicos remontándonos a épocas tan significativas para los católicos como ser la posterior a la creación, la condena de aquel fraude fue el de la serpiente, Eva y la manzana, con las consiguientes secuelas para los descendientes de aquella primera pareja humana. Asimismo indica que hay quienes han afirmado que el fraude ha estado enraizado a todo lo largo de la historia, donde han estado involucrados eminentes representantes sociales desde presidentes de estado, figuras jurídicas, empresarios, sin dejar de lado la hipótesis de que el dinero servía para el financiamiento de actividades ilícitas, como ser el tráfico de sustancias controladas, tráfico de armas y otros.

Es así que el proceso de defraudación empieza no a inspirarse en un reto a la inteligencia, sino en una forma organizada de obtener mayores frutos económicos al precio que sea, por lo cual especialistas norteamericanos justifican el ascenso de esta actividad delictiva con argumentos como ser que el fraude se está convirtiendo en un negocio para las organizaciones delictivas

[50] Rodríguez Z. Juan M., Manual de prevención del Fraude, Esabe Editorial S.A., 1991, Pág.

locales, nacionales e internacionales, siendo necesario para lograr sus objetivos criminales obtener información acerca de las características administrativas y documentales de las organizaciones que eligieron como objetivos de sus propósitos, por eso la popular frase **“QUIEN TIENE LA INFORMACIÓN TIENE EL PODER”**, es valorada no sólo por los delincuentes ajenos a las distintas instituciones públicas o privadas, sino incluso por sus propios directivos o empleados.

La incorporación de los ordenadores en las empresas públicas y privadas dio lugar a la inquietud de la posibilidad de agresiones delictivas, otorgándoseles sistemas de seguridad de acuerdo a la época, es decir, muros de hormigón, barrotes, vigilantes, cámaras de seguridad en razón de que las operaciones informáticas eran de uso interno, no teniendo contacto alguno con el exterior posteriormente el contacto con usuarios externos se efectuó en forma on-line en tiempo real, en ese momento lo más apropiado fue el uso de claves de acceso, pero la intranquilidad sigue latente con el avance tecnológico, sumado a la reducción del tamaño de los ordenadores y el tráfico de información on-line.

Ante la incursión de la informática en todos los ámbitos de la sociedad y más aún en el sistema financiero, reemplazando muchos de los documentos tradicionales en soporte papel, en los que constan las operaciones y saldos de cada uno de los clientes, por "anotaciones en cuenta" o registros lógicos realizados en los sistemas informáticos, sin un soporte en papel o con reflejos en papel meramente informativos o secundarios. De ahí que la doctrina ha centrado el estudio del problema desde el enfoque de las manipulaciones de datos informatizados, estableciéndose como la forma más frecuente de comisión de delitos por medios informáticos.

Al compás de la revolución tecnológica, esta clase de conductas ilícitas se fueron perfeccionando rebasando las fronteras, es decir con una dimensión

mundial, en la que muchas veces la misma sociedad facilita involuntariamente su proyección y comisión como por ejemplo el esfuerzo de regenerar a reclusos bajo un programa de formación informática en la cárcel de Framlingham (Massachusetts), cuyo objetivo era la capacitación de 650 reclusos, pero un tiempo después la policía local detecto que cinco reclusos habían utilizado el ordenador de la cárcel para preparar un sofisticado sistema de juego ilegal y tráfico de droga, obteniendo jugosas sumas de dinero; no es de extrañar que en nuestro país exista solamente en la teoría las denominadas políticas de readaptación social del reo, específicamente en la cárcel de San Pedro gracias a la inquietud de los reclusos pueden acceder a cursos de computación, es decir que deben agruparse para solicitar capacitación, la cual es de manera teórica y no así práctica, pero algunos reclusos pueden contar con un computador que solo tiene programas básicos.

El primer fraude informático[51] con resonancia internacional es aquel que sufrió la Compañía de seguros norteamericana "Equity Funding Life Company" que tenía la actividad de un programa combinado de fondo de inversión y seguro de vida con una alta revalorización y liquidez inmediata, proyecto que no tuvo el éxito esperado, ante ese fracaso de aumentar sus activos el Presidente del Consejo de Administración y sus dos socios elaboraron un plan consistente en emitir pólizas ficticias de seguros de vida a nombre de personas inexistentes, eligiendo a un programador de confianza quien diseño y desarrollo un subsistema denominado "Departamento 99", que era accesible a través de un complejo sistema de claves de acceso que sólo conocía el programador que lo había creado lo mantenía en funcionamiento para él y la alta dirección y que para el resto de la compañía era clasificado como altamente confidencial; la emisión de pólizas falsas fue en aumento y con el fin de dispersar riesgos actuariales y conseguir liquidez, comenzaron a vender las pólizas a compañías

[51] Ob. Cit. Pág. 213-215

reaseguradoras, obteniendo un elevado beneficio económico dado que la emisión de dichas pólizas no llevaba aparejada ningún gasto habitual de las pólizas verdaderas, por lo que todo el dinero obtenido de las reaseguradoras era beneficio limpio. Debido a que la legislación norteamericana exige que las compañías aseguradoras que emiten las pólizas retomen el 90% de las primas del primer año a las reaseguradoras, por lo que la Equity se vio obligada al final del primer año a devolver una suma considerable por las pólizas ficticias, lo que obligó a Goldblum y sus colaboradores a generar más pólizas, por la magnitud que estaba alcanzando el fraude, Goldblum empezó a poner fin a la vida de una serie de sus ficticios clientes y reclamar a las reaseguradoras las indemnizaciones correspondientes, las cuales eran cobradas por la compañía sin que se abonase a ningún beneficiario, pero a denuncia de un ex empleado de la compañía contra la alta dirección de la firma, acusándoles de haber efectuado la emisión fraudulenta de una gran cantidad de pólizas; denuncia que fue investigada, con la noticia de las investigaciones desencadeno una caída en la cotización de las acciones de la Equity en la bolsa de Nueva York, concluyendo con la quiebra de la compañía y la condena de Stanley Goldblum a 8 años en la penitenciaría federal de la Isla McNeil, en Washington y a pagar una multa bastante considerable, en tanto sus dos colaboradores fueron condenados a siete y cinco años respectivamente.

Dada la naturaleza de estas acciones y la evolución de los sistemas informáticos requiere soluciones a la brevedad posible, por la inseguridad de los sistemas que se ven expuestos a una variedad de riesgos, y la asimilación de las nuevas técnicas por los delincuentes, franqueando de esta manera las barreras tecnológicas.

Como dijimos al empezar la presente investigación Bolivia no está exenta de esta clase de delincuencia ya que a continuación transcribiremos las noticias de los periódicos locales en cuanto al fraude informático.

“Destituyen a funcionario por fraude informático”, Ni la tecnología pudo evitar que un funcionario de la Corte de Justicia de Cochabamba[52] y su presunto cómplice alteren, a través de una manipulación informática, el sistema de asignación de procesos a los juzgados civiles, según se desprende de un informe administrativo contra el principal responsable que derivó en una investigación de la Fiscalía.

El auxiliar de apellido Arellano fue sorprendido “in fraganti” por los técnicos de informática de la Corte Superior de Justicia, el 25 de enero, cuando maniobraba la base de datos.

A través de una operación sospechosa para los técnicos se detectó que había ingresado datos duplicados para que el proceso que debía recaer en el Juzgado en lo Civil número 8, se procese en el 10.

Al profundizar la investigación se anotaron más anomalías y se vio que en al menos tres casos se manipuló el sistema IANUS a veces con ayuda de su cómplice un Ingeniero de Sistemas, que con sus vastos conocimientos en Informática logro romper las barreras de seguridad de dicho sistema, cabe resaltar que el Sistema IANUS es el programa informático que utiliza el Poder judicial para el Sorteo de Causas ingresadas a los distintos Juzgados.

La Unidad de Régimen Disciplinario del Consejo de la Judicatura destituyó el 31 de marzo al auxiliar de la unidad de Ingreso y Sorteo de Causas, al hallar suficientes elementos de que el funcionario y su cómplice, incurrieron en una falta grave prevista en el artículo 40 de la Ley 1817, numeral tres.

Según el Consejo de la Judicatura, los responsables cometieron un delito y dañaron la imagen de la administración de justicia, por lo que, el expediente fue remitido a la Fiscalía. **(Por Redacción Central - Los Tiempos - 13/04/2010).**

[52] Ver anexos

Con la lectura de esta publicación uno se da de cuenta que ni la entidad que está encargada de administrar justicia en el país está a salvo de los fraudes informáticos.

Otro de los casos es el siguiente "**Banco Bisa deslinda culpa en fraude informático",** La Paz, 28 de jul. El banco Bisa deslindó responsabilidades en el caso de fraude informático denominado "phishing" y asegura que los clientes timados facilitaron la labor de los delincuentes al brindar información[53], indicó Erbol en base a un comunicado de la entidad financiera.

El mismo señala que "de forma fraudulenta y a través de correos electrónicos, los delincuentes lograron obtener información confidencial de algunos clientes, quienes proporcionaron datos personales como el nombre de usuario, las claves secretas y los números de las tarjetas de coordenadas, facilitando así la acción delictiva. Es decir, que esos clientes han permitido que los delincuentes accedan a las claves de ingreso de sus cuentas por Internet".

El Bisa asegura que los sistemas, en todas las redes y los canales de servicios que ofrece son totalmente seguros y aclara que no solicita información confidencial a sus clientes. **(Por Redacción Central – Pagina Siete - 28/07/2011).**

Pero el mas alarmante caso es el siguiente**: "Fiscalía investiga millonario fraude informático bancario, Una funcionaria del Banco Ganadero es buscada por presunta apropiación indebida".**

Un caso de fraude informático por aproximadamente 500.000 dólares es investigado por la Policía desde el 22 de marzo. La jefa de plataforma de la entidad afectada, Ana María C. C., es buscada y sindicada de estafa y

[53] Ver anexos

manipulación informática.

De acuerdo con el cuaderno de investigaciones, el pasado 21 de marzo, la cliente Elsa T. P. presentó un reclamo por el débito de más de 110.000 dólares de su cuenta de ahorro sin su autorización ni firma. Denuncia que fue verificada y constatada por la casa matriz de la entidad financiera con sede en Santa Cruz.

Después de una auditoría interna, la Gerencia del Banco Ganadero identificó a la presunta responsable del desvío de fondos de ésa y otras cuentas cuyos titulares desconocían esos movimientos. Las transferencias fueron efectuadas entre febrero y marzo de 2011.

De acuerdo con los comprobantes de débito, a los que La Prensa tuvo acceso exclusivo, se evidenció que la funcionaria realizó cuatro traspasos de cuenta por 91.318 dólares de una; $ 3.099, de otra, y 5.315 de una tercera, el 10 febrero; y 9.415 dólares el 11 de febrero.

Posteriormente, estas sumas fueron retiradas con firmas y cédulas de identidad falsas en complicidad con otro funcionario, cajero, que fue citado a declarar ante la Fiscalía y actualmente es investigado.

Las Cámaras. La gerencia del Banco Ganadero de La Paz descubrió, a través de una investigación interna hecha con cámaras de seguridad, que fue la misma funcionaria quien realizó los desvíos y retiros de dinero de las ventanillas de la entidad.

Por ese motivo, esa casa bancaria presentó una denuncia en contra de la sindicada por los delitos de estafa, manipulación informática, hurto, falsificación de documento privado y uso de instrumento falsificado, que se procesa

actualmente.

Un investigador de la FELCC comentó que el banco no fue intervenido aún por el ente regulador del Estado. Se presume que el monto del fraude económico es superior a los 500.000 dólares.

El efectivo lamentó la poca cooperación que recibe de los ejecutivos de esta entidad bancaria para llevar adelante su labor investigativa sobre el caso.

Rolando Alípaz Galarza, gerente del Banco Ganadero en La Paz, no quiso referirse al tema y dijo que no está autorizado para brindar información. “No puedo dar información a los medios. Todos los detalles son canalizados en Santa Cruz”.

Entretanto, voceros de la Autoridad de Fiscalización del Sistema Financiero (ASFI) afirmaron desconocer la existencia de un fraude o estafa en el Banco Ganadero de La Paz.

Para destacar, En febrero, la funcionaría del banco realizó las transacciones en complicidad con un cajero.

La gerencia del Banco Ganadero ya tiene conocimiento del caso, pero no informa.

La abogada de la entidad financiera está de vacaciones y el caso está paralizado en la Fiscalía.

Cifras importantes, 5 meses han transcurrido desde que la funcionaria fue descubierta y desapareció luego de que se detectara la estafa en el Banco Ganadero de La Paz.

36 mil dólares recuperaron los policías del domicilio en el que habitaba Ana María C. C., en la zona de San Miguel, en un allanamiento de la Policía. **(EL DIARIO 07-08-2011).**

Aquí se demuestra con claridad la falta de tipicidad del fraude Informático en el Código Penal boliviano ya que a la Sra. Ana María C. C., la Fiscalía le esta imputando por dos delitos ESTAFA y MANIPULACION DE DATOS, y puesto que ya transcurrieron 5 meses del hecho, las autoridades llamadas por ley no han tenido avance alguno, esto a mi parecer se debe a lo complejo que resulta de subsumir dos delitos distintos en un solo hecho, lo cual es perjudicial y hasta a veces muy difícil para los operadores de justicia en nuestro país, pero este tema de la dificultad de subsunción se tocara en un capítulo más adelante.

Ahora veremos una publicación del periódico OPINION el cual, a manera de queja menciona que en el país no tenemos una Ley expresa sobre delitos informáticos, por lo cual para nuestras autoridades llamadas por ley es muy difícil sentar precedentes para los cibercriminales, **"BOLIVIA SIN LEYES PARA DELITOS INFORMÁTICOS"**, En Bolivia los delitos informáticos son tratados como delitos comunes, están incluidos en el Código Penal y no tienen una ley específica[54].

Haciendo relación a las leyes que se pretendían aprobar en países como Estados Unidos, en Bolivia no existe ninguna normativa de este tipo.

En temas de cibercriminalidad se presentan casos de hackers que intervienen portales de internet como los de las entidades financieras.

Ante la identificación de hechos delictivos relacionados a la intervención de

[54] Ver anexos

páginas web para ejecutar estafas financieras “fraude informáticos” se hace cargo de las investigaciones la División de Económicos y Financieros de la Fuerza Especial de Lucha Contra el Crimen (FELCC).

Tampoco existe ningún proyecto de ley que se haya presentado ante la Asamblea Legislativa Plurinacional y que se refiera a los contenidos que circulan en internet.

El diputado de Convergencia Nacional, Mauricio Muñoz, considera que ya existe jurisprudencia a nivel internacional sobretodo en países que tienen tecnología avanzada.

Pero también agrega que a medida que avanza la tecnología en internet también avanzan las infracciones que se cometen.

“No solamente en el ámbito de los derechos de propiedad intelectual de autoría, sino también existen delitos financieros que se manejan a través de la tecnología”, expresa Muñoz.

La autoridad considera que deberían existir leyes que reglamenten y que pongan un freno a delitos financieros que se registran por ejemplo en el robo de tarjetas de crédito o de dinero a través de hackers que intervienen portales y acceden a la información confidencial.

“En este momento no existe una ley como tal, pero sí se considera delitos penales comunes, los ataques de manera informática a cuentas bancarias para disponer y transferir dineros”, describe el parlamentario.

Para los denominados “cibercriminales” asaltar, por ejemplo, entidades financieras no requiere de las armas de fuego, ni se registran heridos. Los

atracos virtuales son ejecutados por hackers que logran acceder a la información confidencial de las entidades para conseguir códigos de tarjetas y de cuentas bancarias causando después daños económicos graves.

El responsable de la División de Económicos y Financieros de la FELCC, capitán Juan José Blanco, explica que la Policía recibe las denuncias de este tipo de manera verbal o escrita, o con las querellas respectivas ante el Ministerio Público.

Durante la gestión 2011 se presentaron casos aislados referentes a este tipo de delitos y en lo que va de 2012 no existen casos de esa naturaleza registrados.

En julio de 2011 dos personas fueron remitidas a cárceles en Cochabamba por haber incurrido en estos hechos manipulando datos informáticos e interveniniendo la página web de una entidad financiera. Accedieron a cuentas bancarias y lograron cobrar cheques causando un daño de cerca a 50 mil dólares.

“Para este tipo de casos la investigación es amplia y no sólo nos enmarcamos a los conocimientos que puedan tener los investigadores especiales, sino que se acude a peritos”, expresa la autoridad policial refiriéndose a la necesidad de acceder a la colaboración de gente experta en otras áreas para las investigaciones de este tipo de delitos.

Para seguir procesos por estos casos, según la normativa vigente, la Policía Boliviana y el Ministerio Público acuden a los peritos informáticos que tienen vasta experiencia en el tema.

“Los policías, los jueces, los fiscales y toda autoridad llamada por ley no puede saberlo todo y requerimos al conocimiento, oficio, ciencia, arte de otras

personas”, agrega. **(Por: MELISSA REVOLLO mrevollo@opinion.com.bo 29/01/2012).**

Al respecto de las publicaciones transcritas debemos abordar la doctrina de expertos en el tema, es así que veremos lo que significa el fraude para los autores chilenos Magliona y López, estos mencionan que el fraude informático es uno de los fenómenos más importantes dentro de la delincuencia informática, dado al creciente aumento de las manipulaciones fraudulentas, es por tanto la zona más inexplorada y la que mayores problemas enfrenta en cuanto a su prevención, detección y represión.

Estas nuevas formas de delincuencia y la falta de respuesta legal adecuada, ha constituido una realidad común en todos los países, al verse sorprendidos por el desarrollo de un fenómeno cuya progresión no se había previsto, por lo cual la tendencia ha sido la protección jurídica ante las nuevas tecnologías, por su grado de dificultad en el descubrimiento de la dinámica del fraude y de su autor acoplando a ello el desinterés de los afectados en su persecución.

Es innegable que los ilícitos patrimoniales que se cometen a través de medios informáticos denominados fraudes informáticos, por su peculiar dinámica comisiva en la que el sistema informático es el instrumento o el medio a través del que se produce el hecho lesivo del patrimonio ajeno, hace público la vulnerabilidad de sistemas que tienen gran interés en presentar como inexpugnables, causando perjuicios superiores a los que provoca la delincuencia "tradicional".

3.2. EL FRAUDE INFORMATICO

El Fraude Informático es apreciado como aquella conducta consistente en la manipulación de datos, alteración o procesamiento de datos falsos contenidos en el sistema informático, realizada con el propósito de obtener un beneficio

económico. Pero para un mejor entendimiento el fraude informático es inducir a otro a hacer o a restringirse en hacer alguna cosa de lo cual el criminal obtendrá un beneficio por lo siguiente:

1. Alterar el ingreso de datos de manera ilegal. Esto requiere que el criminal posea un alto nivel de técnica y por lo mismo es común en empleados de una institución pública o privada que conocen bien las redes de información de la misma y pueden ingresar a ella para alterar datos como generar información falsa que los beneficie, crear instrucciones y procesos no autorizados o dañar los sistemas.
2. Alterar, destruir, suprimir o robar datos, un evento que puede ser difícil de detectar.
3. Alterar o borrar archivos.
4. Alterar o dar un mal uso a sistemas o software, alterar o reescribir códigos con propósitos fraudulentos. Estos eventos requieren de un alto nivel de conocimiento.

Otras formas de fraude informático incluye la utilización de sistemas de computadoras para robar bancos, realizar extorsiones o robar información clasificada.

Estas conductas consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas.

Los distintos métodos para realizar estas conductas se deducen, fácilmente, de la forma de trabajo de un sistema informático: como por ejemplo es posible alterar datos, omitir ingresar datos verdaderos o introducir datos falsos, en un ordenador. Esta forma de realización se conoce como manipulación del input.

3.2.1. CONCEPTO DE FRAUDE INFORMÁTICO

Para Romeo Casabona[55], el fraude informático, es la incorrecta modificación del resultado de un procesamiento automatizado de datos, mediante la alteración de los datos que se introducen o ya contenidos en el ordenador en cualquiera de las fases de su procesamiento o tratamiento informático, con ánimo de lucro y en perjuicio de un tercero.

En nuestro criterio, fraude informático “es el conjunto de conductas dolosas que se vale de medios fraudulentos para realizar la manipulación informática de datos en un sistema informático, con ánimo de lucro, produciendo un perjuicio económico a un tercero.

En el concepto señalado se hace referencia a las manipulaciones de datos (fase Input) como a las manipulaciones de salida (fase output), Cabe señalar también que menciona que se debe tomar en cuenta que dichas manipulaciones también pueden ser realizadas en forma distinta, por ejemplo, a distancia y en cajeros bancarios automáticos.

En síntesis lo relevante es que la acción del sujeto activo vaya encaminada a la modificación del resultado de un procesamiento automatizado de datos, para así lograr un enriquecimiento injusto en detrimento del patrimonio de un tercero, hay una apropiación ilícita de dinero, bienes o servicios ajenos. Al respecto los autores Chilenos Magliona y López mencionan que debe tratarse de un perjuicio cuantificable, tangible. Esto a diferencia de Luís Camacho Losa el cual al referirse a los perjuicios originados por el sujeto activo, les otorga un sentido amplio, ya que puede tratarse de perjuicios económicos directos (como la apropiación de bienes); perjuicios económicos indirectos (como por ejemplo la sustracción de información confidencial de carácter económico, comercial, etc.);

[55] En http://www.monografias.com

y perjuicios económicos intangibles (por ejemplo, repercusiones sobre la imagen o el prestigio de una organización), dicha posición es la más adecuada, pero siempre hay que tener en cuenta que los perjuicios causados por el fraude informático son netamente de carácter económico.

3.2.2. NOCIÓN DE FRAUDE Y DEFRAUDACIÓN

Para entender el fenómeno de fraude informático, es preciso estudiar o analizar en primer lugar los datos básicos que son la noción de fraude así como lo informático.

Toda vez que el término fraude con frecuencia suele identificarse con la idea de engaño, aunque no puede ser cualquier engaño o ardid, sino que debe gozar de cierta idoneidad y eficacia valorativa para producir la lesión patrimonial. El tratadista ecuatoriano Jorge Zabala Baquerizo[56] indica que el fraude es un modo de actuar dentro de la vida, una conducta que se manifiesta, unas veces, mediante el engaño y en otras mediante el abuso de confianza.

Juan Rodríguez[57] define al fraude como todo engaño o acción de mala fe ejecutada con el fin de procurarse un beneficio ilícito en perjuicio y a expensas de otro o el acto o efecto de lesión que se causa en el patrimonio ajeno de forma no violenta, por medio de engaño y con intención de lucro. Se consuma cuando el bien sustraído pasa a manos del culpable aunque no se haya producido todavía el lucro. Por tanto, cuando se habla de fraude se está aludiendo al modus operandi, a la dinámica intelectiva, que caracteriza un determinado comportamiento, es decir que ese accionar mediante el despliegue de medios engañosos, desencadena en la vulneración del acervo patrimonial

[56] En http://delitosinformaticos.com/trabajos
[57] Ob. Cit. Pág. 21

del sujeto pasivo mediante su inducción al error. Podemos deducir que el engaño (Animus Decipiendi), es la máxima expresión del fraude así como el empleo de artificios, ardid o medios intelectuales para la elaboración de maquinaciones eficientes.

Otro elemento necesario para que se configure el fraude, es la existencia de una lesión o la puesta en peligro de un bien jurídico protegido. Doctrinalmente el bien jurídico protegido por las defraudaciones es el patrimonio, considerado este como el conjunto de bienes que pertenecen a una persona y que son evaluables económicamente se ejerza o no sobre ellos dominio, Cabanellas refiere que es el conjunto de bienes, créditos y derechos de una persona y su pasivo, deudas u obligaciones de índole económica[58]. Por tanto cuando se utiliza la formula fraude se hace en relación con específicos bienes jurídicos lesionados o puestos en peligro.

Entonces la defraudación es el perjuicio económico ocasionado mediante fraude, el cual comprende no sólo el engaño y el abuso de confianza sino también el uso de otros medios fraudulentos, que no solo afectan el patrimonio individual de una persona, sino que también lesionan otros intereses económicos de carácter macro social.

Esta definición de defraudación es la que se ha tomado como la más apropiada, al ser una definición amplia y que reúne a una multiplicidad de conductas defraudatorias realizadas por medio de comportamientos sutiles, falaces, y sagaces que tienen el propósito de conseguir una ventaja económica.

3.2.3. CARÁCTER INFORMÁTICO DEL FRAUDE

[58] Cabanellas Guillermo, Diccionario Enciclopédico de derecho usual, Tomo VI, 27° edición, editorial Heliasta; Pág. 152.

El carácter informático del fraude alude al instrumento con cuyo auxilio se efectúa la conducta delictiva, es decir que se habla de la utilización de sistemas Informáticos como instrumento para perpetrar una conducta astuta, engañosa, maliciosa, artera con el animus decipiendi.

Entonces para hablar de fraude informático debe tener las notas características y configuradoras de una defraudación, es decir que debe existir la comisión de un perjuicio económico, irrogado mediante un comportamiento engañoso, astuto, artero, o sea un, medio fraudulento que en este caso sería la propia manipulación informática.

Para Magliona y López esto es muy importante ya que ayuda a distinguir el fraude informático de otros hechos delictivos, que no obstante de ser realizados por medios informáticos, no constituyen defraudaciones, por ejemplo, atentados contra la intimidad cometidos por medio de manipulaciones informáticas. A este respecto Marcelo Huerta y Claudio Líbano[59], señalan que la finalidad perseguida por el sujeto activo, es la que condiciona el tipo de delito que se produce, ya que para ellos las manipulaciones informáticas se aplican a todos los delitos informáticos.

Al respecto si bien la finalidad del sujeto activo ayuda a conocer qué tipo de delito se comete, así como el aprovechamiento de las características y peculiaridades de los sistemas de procesamiento automatizado de datos es una característica común en todos los delitos informáticos, dichos supuestos no pueden cambiar la naturaleza del hecho delictivo en tal razón y siguiendo a la tratadista española Gutiérrez Francés “nada será defraudación informática sin ser antes defraudación".

[59] Ob. Cit. Pág. 125

3.3. TIPOS DE FRAUDE INFORMATICO MAS CONOCIDOS

3.3.1. EL CABALLO DE TROYA (TROYAN HOURSE).

El término "caballo de Troya" proviene de una fábula griega, en la que los griegos presentaron un gigantesco caballo de madera a los troyanos como una ofrenda de paz. Sin embargo, una desagradable sorpresa esperaba a los troyanos al ver como los soldados griegos salían del caballo hueco y capturó Troya. Del mismo modo, un programa caballo de Troya se presenta como un programa de computadora útil, mientras que en realidad causa estragos y daños a su ordenador.

Cada vez más, los troyanos son la primera etapa de un ataque y su objetivo primordial es mantenernos escondidos durante la descarga y la instalación de una amenaza más fuerte, como un robot. A diferencia de los virus y gusanos, los caballos de Troya no pueden propagarse por sí mismos. A menudo llegan a la víctima a través de un mensaje de correo electrónico en el que se disfraza como una imagen o una broma, o por un sitio web malicioso, que instala el troyano en un ordenador a través de vulnerabilidades en el software del navegador web, como Microsoft Internet Explorer.

Una vez instalado, el troyano se esconde en silencio en la máquina infectada, invisible llevar a cabo sus fechorías, como la descarga de spyware, mientras la víctima continúa con sus actividades normales.

3.3.2. EL SPYWARE

El spyware es un término general usado para los programas que, en secreto supervisan su actividad en su computadora, la recopilación de información personal, como nombres de usuario, contraseñas, números de cuenta, archivos, e incluso la licencia de conducir o números de seguridad social. Algunos programas de spyware se centra en el monitoreo del comportamiento de una persona a Internet, este tipo de software espía a menudo un seguimiento de los lugares que visitar y cosas que hacer en la web, los correos electrónicos que escribe y recibir, así como sus conversaciones de mensajería instantánea (E-MAIL). Después de recoger esta información, el software espía luego transmite esa información a otro ordenador, por lo general con fines publicitarios.

El spyware es similar a un caballo de Troya en el que los usuarios sin saberlo, realizan la instalación del producto cuando instalan otra aplicación. Sin embargo, aunque este software es casi siempre desagradable, puede ser utilizado en algunos casos para la vigilancia en conjunción con una investigación.

El spyware se instala la mayoría de las veces sin saberlo, el software espía se instala con otro software que el usuario desea instalar. Por ejemplo, si instala un "libro" de música o un servicio para compartir archivos o descargar un protector de pantalla, también puede instalar spyware. Algunas páginas Web intentan instalar spyware cuando usted visita su página de manera que usted no se da de cuenta.

3.3.3. EL PHISING (PESCA)

Phishing (pesca) es un término informático que denomina un tipo de delito encuadrado dentro del ámbito de los fraudes informáticos, y que se comete

mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El estafador, conocido como phisher (pescador), se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.

Hoy en día no es raro escuchar por la radio y televisión comerciales de entidades bancarias, advirtiendo sobre este tipo de fraude informático a sus clientes, indicando que no deben dejar que nadie los sorprenda ni tampoco deben dar a nadie datos referidos a cuentas bancarias y que si alguien es víctima de este tipo de delincuente debe comunicarlo enseguida.

3.3.3.1. TÉCNICAS DE PHISHING

La mayoría de los métodos de phishing utilizan alguna forma técnica de engaño en el diseño para mostrar que un enlace en un correo electrónico parezca una copia de la organización por la cual se hace pasar el impostor. URLs *(localizador de recursos uniforme, más comúnmente denominado URL, sigla en inglés de uniform resource locator)* mal escritas o el uso de subdominios son trucos comúnmente usados por phishers, como el ejemplo en esta URL, http://www.nombredetubanco.com/ejemplo. Otro ejemplo para disfrazar enlaces es el de utilizar direcciones que contengan el carácter arroba: @, para posteriormente preguntar el nombre de usuario y contraseña (contrario a los estándares). Por ejemplo, el enlace http://www.google.com@members.tripod.com/ puede engañar a un observador casual y hacerlo creer que el enlace va a abrir en la página de www.google.com, cuando realmente el enlace envía al navegador a la página de members.tripod.com (y al intentar entrar con el nombre de usuario de www.google.com, si no existe tal usuario, la página abrirá normalmente). Este

método ha sido erradicado desde entonces en los navegadores de Mozilla e Internet Explorer. Otros intentos de phishing utilizan comandos en Java Scripts para alterar la barra de direcciones. Esto se hace poniendo una imagen de la URL de la entidad legítima sobre la barra de direcciones, o cerrando la barra de direcciones original y abriendo una nueva que contiene la URL ilegítima.

En otro método popular de phishing, el atacante utiliza contra la víctima el propio código de programa del banco o servicio por el cual se hace pasar. Este tipo de ataque resulta particularmente problemático, ya que dirige al usuario a iniciar sesión en la propia página del banco o servicio, donde la URL y los certificados de seguridad parecen correctos. En este método de ataque (conocido como Cross Site Scripting) los usuarios reciben un mensaje diciendo que tienen que "verificar" sus cuentas, seguido por un enlace que parece la página web auténtica; en realidad, el enlace está modificado para realizar este ataque, además es muy difícil de detectar si no se tienen los conocimientos necesarios.

Otro problema con las URL es el relacionado con el manejo de Nombre de dominio internacionalizado (IDN) en los navegadores, puesto que puede ser que direcciones que resulten idénticas a la vista puedan conducir a diferentes sitios (por ejemplo dominio.com se ve similar a dominio.com, aunque en el segundo las letras "o" hayan sido reemplazadas por la correspondiente letra griega ómicron, "o"). Al usar esta técnica es posible dirigir a los usuarios a páginas web con malas intenciones. A pesar de la publicidad que se ha dado acerca de este defecto, conocido como IDN spoofing o ataques homógrafos, ningún ataque conocido de phishing lo ha utilizado.

3.4. OTROS FRAUDES INFORMATICOS

Entre otros Fraudes Informáticos tenemos:

3.4.1. FRAUDE POR MANIPULACIÓN EN EL INGRESO DE DATOS

Este tipo de fraude informático conocido también como **DATA DIDDLING** consiste en la introducción de datos falsos al computador con el objeto de defraudar, es decir obtener beneficios económicos, la falsedad de los datos puede ser en forma total o parcial o en su caso puede omitirse para lograr una deformación de la realidad, donde el sistema verificará de manera normal los datos falsos que fueron introducidos produciendo un resultado correcto, como ejemplo en Bolivia se tiene la detención de los primeros Hackers identificados como Horacio Pablo Villarreal y Marco Antonio Aguilar quienes eran funcionarios de Impuestos Internos, su modus operandi consistía en alterar las cifras de los aportes de los contribuyentes, por ejemplo de una "X" empresa que pagaba 24.000 Bs. por sus impuestos estos hacían aparecer en la computadora sólo 4.000Bs., con un daño económico al Servicio de Impuestos Internos de más de 200.000 bolivianos, asimismo la PTJ (nombre de la FELCC de ese tiempo) no descarto que el hecho tuviera relación con el robo de impuestos a comunicaciones illimani- ATB, colegios particulares de La Paz.[60]

3.4.2. FRAUDE POR MANIPULACIÓN Y MODIFICACIÓN DE PROGRAMAS

En este tipo de manipulaciones parte de un ingreso correcto de datos, posteriormente se puede modificar los programas existentes en el sistema de computadoras, insertar nuevas rutinas o eliminar algunos pasos del programa, el objetivo es lograr un resultado incorrecto.

[60] El Nuevo Día, 16 de marzo de 2010, pág.2b

Cabe resaltar que por su naturaleza de estas conductas cuando son bien realizadas son difíciles de detectar, ya que no dan señales para su detección y alertar a los encargados de seguridad, pero este tipo de accionar generalmente pasan inadvertidas porque son realizadas mediante modificaciones sencillas y mínimas en la estructura del programa.

Entre esta clase de manipulación tenemos a:

3.4.2.1. LA TECNICA DEL SALAMI O ROUDING DOWN

Traducido como redondeando abajo o técnica del salami, consiste en la introducción o modificación de ciertas instrucciones de ejecución en un programa con el objetivo de extraer pequeñas cantidades de dinero, puede ser también por el redondeo de cuentas aproximando las centésimas a la unidad, produciendo de esta manera que los asientos contables cuadren, situación que convierte a estos ilícitos en simples y de complejo descubrimiento, conocido también como "robo hormiga" técnica en la cual el delincuente modifica un sistema informático financiero para que desvíe pequeñas cantidades de dinero a una cuenta fantasma.

3.4.2.2. EL SUPERZAPPING

El nombre procede del vocablo superzap (superllave) que corresponde al programa utilizado como una herramienta del sistema, capaz de superar todos los controles a fin de introducirse por motivos de emergencia en el punto que se desee.

Es decir consiste en la utilización fraudulenta de un programa, con el fin de alterar los datos contenidos en un programa, la clave de este accionar es que la alteración de datos se lo atribuye a un mal funcionamiento de los equipos o a

transacciones equivocadas, asimismo no guarda ningún registro de las maniobras realizadas para la alteración de los datos en beneficio del autor o de un tercero.

3.4.3. MANIPULACIÓN DE LOS DATOS DE SALIDA

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

3.5. COMERCIO ELECTRÓNICO Y FRAUDE INFORMATICO

El tránsito del comercio tradicional hacia el comercio electrónico con transacciones soportadas electrónicamente remplazando el papel por códigos binarios y la inclusión de la firma electrónica no es una tarea fácil, por los riesgos que se asumen y la reacia confianza de los usuarios por los innumerables casos de fraudes.

En Bolivia con la implementación de la tecnología las actividades empresariales, Industriales, comerciales alcanza a un 85% y el 70% con conexión en redes, constituyéndose la tecnología en la herramienta necesaria para las empresas para mejorar su productividad y eficiencia, dando lugar a que los negocios tengan una vitrina virtual con productos nacionales como es el

caso de BoliviaMall.com que vende más de 3000 productos, trabajando con artesanos y empresas, cuyas ventas son a nivel nacional e internacional a diferencia de Bolivia.com. Que solo lo realiza a nivel nacional.

El Banco Nacional amplia las plataformas para el comercio electrónico, presentando el 15 de octubre de 2002, su nuevo portal financiero asegurando que es la renovación del sitio original y que sus clientes podrán satisfacer sus necesidades financieras desde sus hogares y oficinas, permitiendo realizar transacciones vía Internet, simuladores de préstamos y depósitos, teniendo entre 80 mil a 100 mil transacciones mensuales, unos dos millones y medio de transacciones, esta realidad demuestra que en Bolivia hay un fuerte uso de la tecnología y de redes como Internet

Con la conexión a las redes informáticas internas y/o externas las empresas, banca e industria se constituyen en posibles víctimas de audaces sujetos que con algún conocimiento de informática logran obtener ventajas económicas, burlando los sistemas de seguridad, los sujetos activos como se estudio en capítulos precedentes pueden ser personal de la misma institución o ajenos a ella, manipulando los sistemas como lo realizado por dos funcionarios de Impuestos Internos obteniendo una ganancia ilícita de Bs. 200.000 aproximadamente. Otra forma de fraude informático por manipulación de los programas es lo sucedido a clientes del Banco de Crédito quienes indicaron que a momento de retirar dinero de los cajeros automáticos este debitaba de la cuenta el monto requerido pero no realizaba la entrega del dinero comenzando ahí su calvario.

Por lo brevemente explicado el comercio electrónico se realiza con extrema precaución, pero esta nueva forma de comercializar productos conduce a que se den fraudes informáticos por lo que es necesaria una regulación más adecuada en nuestro país.

3.6. ESTAFA Y FRAUDE INFORMÁTICO DIFICULTAD DE SUBSUMIR UN DELITO EN EL OTRO

El Artículo 335 del Código Penal[61], recoge el tipo de la estafa el cual dice:

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 a cinco años y con multa de sesenta a doscientos días[62].

La estafa es un delito por el cual una persona mediante fraude (engaño, o abuso de confianza) y con ánimo de apropiación induce a otra a entregarle una cosa de su propiedad o de un tercero, elementos que constituyen al delito de estafa, los mismos que deben ser examinados con el fin de determinar si se puede subsumir en su estructura al fraude informático, concepto que abarca las características tanto objetivas (como el fraude y la entrega de la cosa) como subjetivas (dolo y animo de apropiación) contenidas en el Art. 335 del código Penal boliviano.

El engaño realizado por el autor basado en apreciaciones falaces deben estar acompañadas de actos aptos para inducir a engaño, asimismo el animus decipiendi tendiente a hacerse entregar una cosa ajena consuma el delito de estafa. Este elemento subjetivo tanto en la estafa como en el fraude informático está presente, ya que en ambos casos el ánimo del sujeto activo quiere

[61] Extrayendo parte del Art. 335 del Código Penal Boliviano, que señala "…mediante engaños o artificios provoque o fortalezca error en otro que motive la realización de un acto de disposición patrimonial…".
[62] Código Penal Boliviano

apropiarse de algo que le es ajeno, que no le pertenece, por tanto con la acción ejecutiva lo que se persigue es lesionar el patrimonio ajeno.

Para los delitos contra la propiedad el objeto jurídico o el bien jurídico protegido es la propiedad en su sentido más amplio, es decir a la propiedad considerada como: el derecho o facultad de gozar, poseer y disponer de una cosa sin más limitaciones que las establecidas en las leyes.

Para el profesor Zabala Baquerizo[63], el fraude se presenta únicamente de dos formas el engaño y el abuso de confianza. En cuanto al dolo señala que “La esencia de la estafa radica en que el agente actúa con la intención de engañar o abusar de la confianza de la victima para lograr que ésta disponga del bien del cual se desea apropiar el agente".

La dificultad que presenta la estafa para encasillar al fraude informático, es la de extender el concepto del engaño a un computador para obtener un ventaja económica, es decir que el empleo de manejos fraudulentos siempre irán dirigidos o al engaño o al abuso de confianza de la víctima (tomando en cuenta la intención del agente), lo que hace imposible la adecuación del tipo penal de la estafa al fraude informático dado que no es factible engañar o hacer caer en el error psicológico o abusar de la confianza de una máquina.

Por tanto diremos que en el fraude informático, existe la utilización de un medio doloso para la comisión de la infracción que es a saber, la manipulación informática fraudulenta y que la intención del agente va dirigida en primer lugar a causar un perjuicio económico a la víctima y en segundo lugar está el ánimo de lucro con el cual este actúa, en este punto hay que tener muy en cuenta la relación de causalidad que tiene el delito de estafa y el fraude informático, en el primero la relación de causalidad esta dado por el engaño o el abuso de

[63] En http://delitosinformaticos.com/trabajos

confianza que utiliza el sujeto activo de la infracción como medio para lograr el error psicológico en el sujeto pasivo por el cual éste entrega al agente la cosa corporal mueble que éste quiere apropiarse. En este caso la voluntad de la víctima del delito está viciada por el error causado por el engaño o el abuso de confianza. En el fraude informático la relación de causalidad está dada por la manipulación informática fraudulenta como medio para lograr la disposición patrimonial lesiva, en este caso y a diferencia de la estafa la víctima no expresa voluntad alguna, no existe vicio alguno de la voluntad, por cuanto no existe ni el engaño ni el abuso de confianza, lo que existe es la manipulación informática fraudulenta.

Otra imposibilidad de adecuación del fraude informático al tipo penal de la estafa tiene relación con la disposición que hace la víctima de la cosa corporal mueble que el agente quiere apropiarse. A este respecto dentro del fraude informático no cabe hablar de entrega de la cosa corporal mueble por la siguiente situación que el acto de entregar supone la existencia de una voluntad para hacerlo que como vimos en líneas anteriores existe aunque viciada en la estafa pero no en el fraude informático, dado que lo que existe verdaderamente es una transferencia no consentida de un activo patrimonial lograda a través de una manipulación informática fraudulenta, no existe por tanto entrega material, alguna, sino simplemente un traspaso de fondos entre dos cuentas corrientes que pertenecen a titulares distintos (Agente, Víctima).

Como se ha analizado el dilema de adecuar el fraude informático al tipo penal clásico de la estafa radica en la imposibilidad de engañar a una máquina o de la existencia de un error psicológico por parte del computador que lo lleva a la disposición patrimonial lesiva, por tal razón para la estafa es necesario que participen dos o más personas, únicas en las que pueden concurrir el error y la inducción, en definitiva a las máquinas no se las puede engañar.

Por tales razones y al verse el tipo penal de la estafa desbordado por los nuevos avances tecnológicos aplicados por los delincuentes para efectuar sus defraudaciones, muchos países han dado lugar al nacimiento de un nuevo tipo delictivo, el fraude informático que vendría a absorber todas aquellas conductas de defraudación, que por tener incorporada la informática como herramienta de comisión, no podían ser subsumidas en el tipo clásico de la estafa, a diferencia de nuestra legislación que ha encuadrado en el tipo penal de manipulación informática lo que constituye el fraude informático. Asimismo en la actualidad si bien existen denuncias sobre Fraude Informático, este tipo de delito no está tipificado en nuestro ordenamiento jurídico, y según las entrevistas realizadas a los operadores de justicia, lo que se hace es poner el titulo de dos delitos en un mismo caso, que son ESTAFA y MANIPULACION INFORMATICA, lo cual según criterios de expertos en el tema dificulta de gran manera el avance de estas investigaciones delictivas.

3.7. VACIOS JURIDICOS EN MATERIA DE FRAUDE INFORMATICO EN BOLIVIA

Como indica el Dr. Jaime Moscoso Delgado un acto es delito cuando encaja dentro de una de las figuras descritas en el "supuesto" o "hipótesis" de una ley penal, la cual, en su otro extremo, en la "consecuencia" o "disposición", señala el castigo correspondiente. Desde la imposición del principio de legalidad por el cual no se establece ninguna sanción sin una ley previa, y los Principios Constitucionales establecidos en el Art. 8 de la Constitución Política del Estado.

Podemos concluir que en el Derecho penal pueden existir vacíos jurídicos, porque se rige estrictamente a los principios de legalidad y en caso de inconsistencia u obscuridad de la ley debe aplicarse el principio "lndubio pro

Reo", las denominadas lagunas jurídicas, son casos no previstos por el ordenamiento jurídico vigente, que constituyen vacíos que dejan sin regulación jurídica algunas relaciones sociales.

Ciertos vacíos jurídicos pueden ser cubiertos mediante la integración del derecho que ofrece dos medios: La analogía y los principios generales del Derecho.

Como se establece en la Doctrina Jurídica el derecho penal no recurre a la analogía y Alfonso Arroyo de las Heras en su Manual de Derecho Penal, indica que "la admisión de la analogía supondría una evidente regresión a épocas históricas totalmente superadas y entraña una amenaza al principio de garantía de los derechos individuales, porque, desde un punto de vista meramente técnico, no se conforma con los caracteres de antijurícidad y tipicidad integrantes del concepto mismo del delito" (ARROYO-MUÑOZ: 1980).

Asimismo el Dr. Benjamín Harb en su libro Derecho penal Tomo I establece que cualquiera sea la clase de analogía será rechazada mientras esté vigente el principio de legalidad puesto que deja abierta la puerta para el arbitrio judicial (HARB: 1995), afectando directamente los derechos de los ciudadanos.

De lo cual concluimos que ante una insuficiencia de la ley penal el delito de fraude informático carece de regulación en el caso de establecimiento de responsabilidad a los administradores de la operación de los equipos informáticos y los desarrolladores de software.

Si bien la manipulación informática establece que cualquier persona puede ser sujeto activo del tipo penal, con el único elemento objetivo que es lograr beneficiarse o logre beneficiar a tercero en la manipulación o bloqueo de procesos informáticos, no aclara la posibilidad de que la delincuencia interna o

externa a la organización bancaria se halle estrictamente relacionada con la responsabilidad del gerente del sistema informático o el desarrollador del software.

Como determina el presente estudio el fraude informático siempre puede ser confundido con simples fallas o daños al sistema no autorizados de tal manera que el responsable del sistema puede evadir cualquier responsabilidad por fallo incidental o error involuntario.

Se elude por tanto la acción legal y cualquier responsabilidad penal por la comisión de delitos contra los patrimonios del usuario de la informática.

CAPITULO IV
MARCO JURIDICO

4.1. NUEVA CONSTITUCION POLITICA DEL ESTADO

Nuestra nueva Constitución Política del Estado, no menciona nada acerca de delincuencia informática ni mucho menos lo que es el fraude informático, dada su esencia primordial dentro de las leyes en el estado. Sin embargo en la Sección III menciona el tipo de recurso Constitucional que pueden realizar los ciudadanos respecto a la privacidad la cual es la “Acción de Protección de Privacidad” la cual dice:

ACCIÓN DE PROTECCIÓN DE PRIVACIDAD

Artículo 130.

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.

Artículo 131.

I. La Acción de Protección de Privacidad tendrá lugar de acuerdo con el procedimiento previsto para la acción de Amparo Constitucional.

II. Si el tribunal o juez competente declara procedente la acción, ordenará la revelación, eliminación o rectificación de los datos cuyo registro fue impugnado.

III. La decisión se elevará, de oficio, en revisión ante el Tribunal Constitucional Plurinacional en el plazo de las veinticuatro horas siguientes a la emisión del fallo, sin que por ello se suspenda su ejecución.

IV. La decisión final que conceda la, Acción de Protección de Privacidad será ejecutada inmediatamente y sin observación. En caso de resistencia se procederá de acuerdo con lo señalado en la Acción de Libertad. La autoridad judicial que no proceda conforme con lo dispuesto por este artículo quedará sujeta a las sanciones previstas por la ley.

Claramente en su art. 130 Pfo. I, no se refiere a la Manipulación Informática más bien se refiere a que algunas instituciones públicas o privadas que tuviesen datos de una persona natural o jurídica se negaran a borrarlos, mostrarlos, o

rectificarlos, causando perjuicio a la persona interesada ya sea afectando su privacidad atacando la imagen, honra y reputación de la misma, esta podría utilizar este recurso contra la institución. Simplemente este articulo resalta y quiere hacer prevalecer el derecho a la intimidad y privacidad que tienen las personas.

4.2. LEGISLACIÓN NACIONAL EN MATERIA DE DELITOS INFORMÁTICOS "CODIGO PENAL BOLIVIANO"

Años atrás era tal el desarrollo y avance tecnológico que el derecho positivo no lograba estar acorde con la necesidad de sancionar los ingresos indebidos a los sistemas informáticos, ni las manipulaciones a los mismos sistemas con fines nocivos o patrimoniales. Previendo que no estamos exentos de la velocidad del desarrollo tecnológico y de los vicios que éste genera, en Bolivia el año 1989 se consideró el análisis y tratamiento sobre legislación informática concerniente al flujo de la información computarizada, la necesidad de modernizar los aparatos productivos nacionales, promover la investigación científica tecnológica del país destinado al campo de la informática, así como la necesidad de incorporar en nuestra legislación penal nuevos delitos emergentes del uso y abuso de la informática.

Es así que los legisladores observando el fenómeno informático, viendo que no era posible su regulación por analogía a los tipos penales existentes, buscaron la solución a este problema, optando por la incorporación en el Código Penal dentro del Título XII de los delitos contra la propiedad el capítulo XI denominado Delitos Informáticos, con la inclusión de dos artículos: **363 bis (MANIPULACIÓN INFORMATICA)** y **363 ter. (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS)**, tipos penales en los que se

hace uso de un sistema de computación para llevarse a cabo. Sentando precedente entre los países latinoamericanos como uno de los primeros que cuentan con una legislación que tipifica los ilícitos contra el uso indebido de los datos informáticos en los soportes informáticos.

4.2.1. UBICACIÓN SISTEMÁTICA

En fecha 11 de marzo de l997, el Congreso de la República promulga la Ley Nº 1768, elevando a rango de Ley de la República el Decreto Ley No 10426 de 23 de agosto de 1972 sancionatorio del Código Penal, incorporando los delitos informáticos al Código Penal. Así, Bolivia ingresa a la legislación de los tipos penales relacionados con el desarrollo tecnológico, el nuevo mundo de los delitos informáticos, desconocidos hace más de un par de décadas atrás.

En la regulación de los delitos informáticos el legislador no ha tomado en cuenta la afectación de distintos bienes jurídicos, aglutinando en dos artículos el empleo de medios informáticos, si bien es cierto no es bueno tener leyes extensas si están mal redactadas, tampoco es adecuado que la redacción concentre conductas que puedan dar lugar a una confusión y vacíos importantes.

4.2.2. ANÁLISIS DEL CAPÍTULO REFERENTE A LOS DELITOS INFORMÁTICOS

Su correspondiente análisis constituirá el inicio para la consagración de la debida protección penal de la seguridad informática, para que de este modo se puedan realizar modificaciones e incluso la introducción de nuevos tipos penales al Código Penal, las mismas que son necesarias

Siendo la premisa para que una conducta sea considerada como delito debe contar con los elementos constitutivos, se debe definir el hecho punible de manera inequívoca, de tal manera que la conducta lesione o ponga en peligro sin justa causa el bien jurídico, tomando en cuenta que el resultado del hecho punible debe ser consecuencia de la acción o de la omisión del sujeto quién al momento de ejecutar el hecho antijurídico tenga la capacidad de comprender su ilicitud.

Compartiendo la postura de la doctrina española en el aspecto de reemplazar la denominación “delitos contra la propiedad” con las expresiones "delitos contra el patrimonio o delitos patrimoniales” términos que son los más adecuados para abarcar las distintas figuras que agrupa, debido a que algunos de los tipos no suponen un ataque a la propiedad, sino a la posesión o tenencia; así como los derechos personales, como son los créditos y no un derecho real.

4.2.2.1. MANIPULACIÓN INFORMÁTICA ART. 363 BIS

" 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.[64]”

Nomen Juris.- manipulación del verbo manipular consiste en la acción de operar o utilizar datos de un tercero, mediante el empleo de la informática.

[64] Código Penal Boliviano

Sujeto Activo.- Es impropio, debido a que puede ser cualquier persona que no requiere tener grandes conocimientos de informática.

Sujeto Pasivo.- Indeterminado, puede ser una persona natural o una persona jurídica, titular del bien jurídico protegido.

Bien jurídicamente protegido.- Adecuadamente comprendido dentro de los delitos contra la propiedad, ya que la conducta es la de ingresar, manipular, evitar la concreción de un proceso cuya actividad de por resultado la transferencia patrimonial en perjuicio de un tercero, por lo tanto el bien jurídico protegido son los datos informáticos.

Tipicidad.- Conducta de naturaleza dolosa, se requiere que el agente actúe y lo adecue su accionar con conciencia y voluntad de ingresar o utilizar el elemento informático indebidamente, siendo éste el aspecto subjetivo, porque claramente establece la intención de obtener un beneficio indebido ya sea para sí o de un tercero.

Delito de Resultado.- Es de resultado porque se consuma en el momento de la manipulación de los datos informáticos, obteniendo beneficio económico ilícito.

Este delito nos muestra en primera instancia lo que se denomina hacking y la defraudación realizados a través de un sistema informático, es decir que el legislador articula el ingreso a una base de datos y el método por el cual un sujeto obtiene beneficios económicos para sí o un tercero, su agravante la encontramos en el Art. 346 si se tratare de víctimas múltiples, no se sanciona a aquella persona que por negligencia pueda obtener ganancias ilícitas, no encontrándose la agravante si el Estado fuere la víctima o sujeto pasivo del hecho delictuoso.

4.2.2.2. ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMATICOS ART. 363 TER[65]

"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".

Sujeto Activo.- Es impropio, debido a que puede ser cualquier persona que no requiere tener grandes conocimientos de informática.

Sujeto Pasivo.- Indeterminado, pudiendo ser una persona natural o una persona jurídica.

Bien Jurídicamente Protegido.- El bien jurídico son los datos informáticos.

Tipicidad.- La conducta descrita se refiere a apoderarse, utilizar, acceder, modificar suprimir o inutilizar una base de datos; tratándose de un tipo penal de lesión siendo suficiente que el agente haya ingresado en una base de datos o sistemas informáticos.

Delito Formal.- Porque se consuma en el momento en que ingresa el agente a la base de datos, aun cuando no se haya logrado los resultados deseados, el solo hecho de ingresar a un sistema ya ha generado daño.

Se trata de un tipo doloso el sujeto debe tener la voluntad de ingresar o utilizar el elemento informático, si existiere el desconocimiento por parte del sujeto acerca del carácter indebido de la conducta realizada constituye un error de tipo

[65] Código Penal Boliviano

vencible, cuya solución al tenor de lo establecido por el Art. 16 del Código Penal será la aplicación del tipo penal culposo, pero debido a una inexistencia deberá excluirse de una sanción penal.

En este Artículo el legislador sanciona a aquella persona que no esté autorizada y se apodere, acceda, utilice, modifique, suprima o inutilice datos almacenados en cualquier soporte informático, es decir que no sanciona el accionar de una persona que en función de su cargo este autorizado para acceder a un sistema informático y lo modifique o inutilice, tampoco si el daño pudiera ocasionar un peligro latente en la seguridad nacional.

De manera ambigua se incluye en este Artículo el intrusismo, espionaje y sabotaje informático al indicar primero a quien acceda a los datos almacenados en una computadora, segundo si se apoderare de datos en perjuicio del titular de la información, sin regular que esa información pueda ser divulgada, tercero si modificare o inutilizare datos almacenados en una computadora o soporte informático, sin diferenciar si son datos personales, información empresarial o de la banca, o en su caso afectaren datos que están en los sistemas informáticos del gobierno.

4.4. POSTURA DE DIVERSOS ORGANISMOS INTERNACIONALES EN MATERIA DE REGULACION INFORMATICA

Como se ha indicado en capítulos precedentes una de las características de la delincuencia informática es que puede alcanzar niveles internacionales y que la lucha para enfrentar esta nueva problemática ha conducido a intercambios de opiniones y propuestas de solución tanto por organismos intergubernamentales como por diferentes estados, propuestas que surgen con la posibilidad de

aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra esta delincuencia tecnificada.

La Organización de Cooperación y Desarrollo Económico (OCDE) después de un estudio prolijo en lo concerniente a la diversidad normativa con la premisa de concertar una política legislativa similar para la lucha contra la utilización indebida de los sistemas informáticos, ha publicado en 1986 el informe titulado "Delitos de Informática[66]: Análisis de la Normativa Jurídica" donde se reseñaban las normas legislativas vigentes y las propuestas de reforma de Estados Miembros, asimismo se recomendaba una Lista Mínima que los países podrían prohibir y sancionar en leyes penales por ejemplo el fraude informático, alteración de datos y programas de computadora, sabotaje informático, acceso no autorizado, interceptación no autorizada y la reproducción no autorizada de un programa de computadora protegido. De la misma forma se recomendó una Lista Optativa o Facultativa por la Comisión Política de Información, Computadores y Comunicaciones como espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa de computadora protegido, incluido el robo de secretos comerciales, y el acceso o empleo no autorizado de sistemas de computadoras.

Por su parte el Consejo de Europa inicia estudios sobre el tema con el fin de elaborar directrices dirigidas a colaborar a los legisladores que tipo de conductas debían prohibirse y la forma como debían conseguir ese objetivo. Se fueron añadiendo otras conductas ilícitas a La Lista Mínima preparada por la OCDE, respecto a este tema así como la forma de prevención, procedimiento en la investigación y la confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático.

---

[66] En http://www.stj-sin.gob.mx/

Desarrollada esta fase de análisis, propuestas y directrices planteadas el Consejo de Europa aprobó la recomendación R(99)[67] en la que se "recomienda a los gobiernos de los Estados Miembros que tengan en cuenta cuando revisen su legislación o preparen una nueva, el informe sobre la delincuencia relacionada con las computadoras y en particular las directrices[68] para los legisladores nacionales".

Adicionalmente, en 1992, la OCDE elaboró un conjunto de normas para la seguridad de los sistemas de información, con intención de ofrecer las bases para que los Estados y el sector privado pudieran crear un marco de seguridad para los sistemas informáticos.

La Organización de las Naciones Unidas (ONU) por su parte en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal (Habana -Cuba, 1990) indico que la delincuencia informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países. Siendo necesario adoptar medidas preventivas para prevenir su aumento, en vista de que los delitos informáticos eran un fenómeno nuevo el Congreso recomendó que se establecieran normas y directrices sobre la seguridad de las computadoras a fin de ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia. En el Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos[69] señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos

[67] Esta recomendación fue fue adoptada por el comité de Ministros del Consejo de Europa el 13 de Septiembre de 1999

[68] Estas directrices incluyen una lista mínima de conductas en las que existe consenso sobre su tipificación y que deben incluirse en el derecho penal, así como una lista facultativa en la que se describen los actos que están tipificados como delitos en algunos Estados, respecto a los cuales no han llegado a un consenso internacional a favor de su tipificación.

[69] En http://bufetalmeida.com

constituyen una nueva forma de crimen transnacional y su combate requiere de una eficaz cooperación internacional concertada. Asimismo, la ONU resume de la siguiente manera los problemas que rodean a la cooperación internacional en el área de los delitos informáticos:

- Falta de acuerdos globales acerca de qué tipo de conductas deben constituir delitos informáticos.

- Ausencia de acuerdos globales en la definición legal de dichas conductas delictivas.

- Falta de especialización de policías, fiscales y otros funcionarios judiciales en el campo de los delitos informáticos.

- No armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos.

- Carácter transnacional de muchos delitos cometidos mediante el uso de computadoras.

- Ausencia de tratados de extradición, de acuerdos de ayuda mutuos y mecanismos sincronizados que permitan la puesta en vigor de cooperación internacional.

Por ello han enfatizado que las soluciones puramente nacionales serán insuficientes frente a la dimensión internacional que caracteriza este problema.

En consecuencia, es necesario que para solucionar los problemas derivados del incremento del uso de la informática, se desarrolle un régimen jurídico internacional donde se establezcan las normas que garanticen su compatibilidad y aplicación adecuada y que durante la elaboración de dicho

régimen, se deberán de considerar los diferentes niveles de desarrollo tecnológico que caracterizan a los miembros de la comunidad internacional.

La Asociación Internacional de Derecho Penal durante un coloquio celebrado en Wurzburgo, Alemania, en 1992, adoptó diversas recomendaciones respecto a los delitos informáticos. Estas recomendaciones contemplaban que en la medida en que el Derecho Penal tradicional no sea suficiente, deberá promoverse la modificación de la definición de los delitos existentes o la creación de otros nuevos, si no basta con la adopción de otras medidas (principio de subsidiaridad).

Además, las nuevas disposiciones deberán ser precisas, claras y con la finalidad de evitar una excesiva tipificación.

En síntesis se pretende que las recomendaciones contribuyan a una uniformidad de las normas que sancionan los delitos informáticos en el ámbito internacional, sin que ello signifique dejar la tradición jurídica de cada país.

4.5. DELITOS INFORMATICOS RECONOCIDOS POR LA ORGANIZACIÓN DE LAS NACIONES UNIDAS “ONU”

Los Fraudes cometidos mediante Manipulación de Computadoras que están reconocidos por la ONU. Son:

Manipulación de los datos de entrada, Este tipo de fraude informático, conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir.

Este delito no requiere de conocimientos técnicos de informática y puede

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

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

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

Manipulación informática aprovechando repeticiones automáticas de los procesos de cómputo, Es una técnica especializada que se denomina "técnica del salami o salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.

Falsificaciones informáticas,

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

Como instrumentos: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color a base de rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer copias 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.

Acceso no autorizado a servicios y sistemas informáticos, Por motivos diversos: desde la simple curiosidad, como en el caso de muchos piratas informáticos (hackers) hasta el sabotaje o espionaje informático.

Piratas informáticos o hackers, El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema.

Reproducción no autorizada de programas informáticos de protección legal, Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta

clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, consideramos, que la reproducción no autorizada de programas informáticos no es un delito informático debido a que el bien jurídico a tutelar es la propiedad intelectual.

4.6. POLÍTICAS INTERNACIONALES CONTRA DEL FRAUDE INFORMÁTICO

4.6.1. COMISIÓN FEDERAL DE COMERCIO NORTEAMERICANA (FTC)

La Comisión Federal de Comercio norteamericana (FTC) ha llegado a un acuerdo para trabajar en la lucha contra el fraude en la Red, gracias a esta alianza, todas las partes implicadas recogerán y compartirán información y casos sobre transacciones ilegales que se produzcan en el sector del comercio electrónico. Los 13 países firmantes son: Estados Unidos, Australia, Canadá, Dinamarca, Finlandia, Hungría, México, Nueva Zelanda, Noruega, Corea del Sur, Suiza, Suecia y el Reino Unido.

Además, como parte del proyecto, la FTC ha Lanzado un nuevo sitio web (www.econsumer.gov) disponible en español, inglés, alemán, y francés, donde los consumidores de los 13 países podrán realizar sus quejas y obtener información sobre los fraudes en Internet y qué autoridades defienden al consumidor en cada país.

El incremento del comercio electrónico dio lugar que el fraude on-line aumentara considerablemente en Estados Unidos por consiguiente las denuncias por estafas.

Según un informe presentado por Hugh Stevenson, director asociado de la división de Planificación e Información de la FTC, el número de denuncias en Estados Unidos creció de 10.000 en el año 2007 a 50.000 durante el año pasado.

Entre los fraudes frecuentemente denunciados se encuentran los relacionados con subastas on-line, estafas sobre vacaciones y viajes o cargos a las tarjetas de crédito sin autorización en sitios que ofrecen contenidos para adultos. "Internet ofrece a los consumidores un acceso a productos, servicios e información que se encuentra repartido por todo el mundo, pero esa falta de límites naturales también puede conseguir frustrar el intento de proteger a los consumidores por parte de los gobiernos", señaló Robert Pitofski, presidente de la FTC.

Uno de los países más dedicados a la lucha contra el fraude es Estados Unidos que cuenta con diversas dependencias y organizaciones como ser la: Asociación Americana de Personas Jubiladas (American Association of Retired persons), Oficina Federal de investigación (Federal Bureau of Investigatión), Comisión Federal de Comercio (Federal Trade Comisión), Vigilancia de Fraude por Internet (Internet Fraud Watch), Centro Nacional de Información de Fraudes (National Fraud Information Center), Comisión de Sentencias de los E.U.A. (U S Sentencing Comisión).

4.6.2. CONVENCIÓN SOBRE DELITOS INFORMÁTICOS

Asimismo ente las políticas internacionales tenemos a la Convención sobre Delitos informáticos, el Consejo de Ministros de Europa, compuesto por los Ministros del Interior de los Estados que conforman la Unión Europea, conjuntamente con Estados Unidos, Sudáfrica, Canadá y Japón firmaron en Budapest la Convención sobre Delitos Informáticos.

Constituye sin duda el esfuerzo internacional más importante en contra de las actividades criminales cometidas a través de medios informáticos. La misma tiene lugar en momentos en que el Internet ha dejado de ser tan solo el vehículo más idóneo para la propagación y perfeccionamiento de actos criminales bajo condiciones de anonimato, sino que además representa el entorno más frecuentemente utilizado para la financiación de este tipo de actividades.

Esta Convención, cuya elaboración tomó más de cuatro años, tiene como objetivos fundamentales los siguientes:

a) Armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático;
b) Proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas; y
c) Establecer un régimen dinámico y efectivo de cooperación internacional.

En relación al fraude lo encontramos en la sección I del Capítulo II en el título contempla al fraude informático entendiéndose como tal todo acto ilegítimo e intencional que ocasione la pérdida de patrimonio, cometido a través de la alteración, supresión, eliminación e interferencia de datos informáticos o sistemas de cómputo.

La novedad se encuentra respecto al régimen de responsabilidad penal para las personas jurídicas que estén involucradas en alguna de las conductas descritas en los primeros cuatro títulos. Señalando en su artículo 12 que "cada Estado parte deberá adoptar las medidas legislativas que sean necesarias para asegurar que las personas jurídicas sean responsables penalmente por los actividades delictivas establecidas de conformidad con esta Convención, cometidas en su beneficio por cualquier persona natural que actué ya sea individualmente o como parte de un órgano interno de la misma.

Por todo lo analizado es necesario establecer sanciones y mecanismos de investigación adecuados, que sean lo suficientemente avanzados y dinámicos como para hacer frente a este tipo de actividades delincuenciales que afectan a la raíz misma de nuestra sociedad, la cual es una sociedad que ha llegado a ser denominada por algunos como “sociedad de la información”.

4.7. LEGISLACIÓN COMPARADA

La informática si bien ha servido de puente comunicador entre los avances tecnológicos y el acceso masivo a las diversas fuentes de información, trajo aparejada la aparición de nuevas formas de delinquir, asimismo las innovaciones tecnológicas recientes han revelado la incapacidad experimentada por las normas establecidas por el Derecho Penal tradicional.

La mayoría de los países están haciendo lo posible para incluir en sus legislaciones normas destinadas a proteger la utilización abusiva de la información reunida y procesada así como la difusión de virus o la interceptación de mensajes electrónicos, todo ello con el fin de contar con comunicaciones electrónicas, transacciones e intercambios confiables y seguros.

4.7.1. ALEMANIA

La reforma penal en materia de delitos informáticos, vino como consecuencia de la insuficiencia y deficiencias de las normas tradicionales y los tipos clásicos en ellas previstas. Un largo debate, iniciado a mediados de la década de los setenta, dio como resultado la "Segunda Ley de Lucha contra la Criminalidad Económica" de 1986.

Las modificaciones introducidas por esta Ley en el Código Penal Alemán, respecto de las conductas delictuales relacionadas con los medios informáticos, no sólo consistieron en la modificación de alguna disposición ya existente, sino que en algunos casos se introdujeron nuevas figuras o tipos penales.

Entre las nuevas figuras que regula Ley se encuentran: el espionaje de datos (párrafo 202.a), estafa mediante ordenador o fraude informático (párrafo 263.a), falsificación de datos probatorios (párrafo 269), modificaciones complementarias del resto de las falsedades documentales (párrafo 270, 271, 273, 274 y 348), engaño en el tráfico jurídico mediante sistemas de procesamiento de datos (párrafo 270), modificación de datos (párrafo 303.a) y sabotaje informático (párrafo 303.b).

4.7.1.1. ESPIONAJE DE DATOS.

Párrafo 202.a *"I. Quien consiga sin autorización, para sí o para otro, datos que no le competan y que estén especialmente protegidos contra el acceso ilegítimo será castigado con pena privativa de la libertad de hasta tres años o con multa. II. Datos, a efectos del apartado I, serán sólo aquellos que sean almacenados, transmitido electrónica, magnéticamente, o de forma no inmediatamente accesible".*

El tipo protege el interés formal en el mantenimiento del secreto por parte del titular para disponer del almacenamiento y trasmisión de datos no directamente perceptibles, el que a través de su protección manifiesta su interés en el mantenimiento del secreto. Sujeto activo sólo puede ser aquel para el cual no están previstos los datos, de manera que no contempla el supuesto del empleado que sin autorización utiliza datos que para él son accesibles. La punibilidad está limitada a los datos que están especialmente protegidos contra el acceso no autorizado (ejemplos, contenedores cerrados, contraseñas, encriptados, etc.).

Del concepto de datos del inciso segundo del párrafo 202.a, se desprende que es necesario que el acto de espionaje recaiga sobre datos no perceptibles directamente.

4.7.1.2. ESTAFA INFORMÁTICA.

Párrafo 263.a *"I. Quien, con la intención de procurar para sí o para un tercero una ventaja patrimonial ilícita, perjudique el patrimonio de otro influyendo en el resultado de un proceso de elaboración de datos por medio de una errónea configuración del programa, por medio del uso de datos incorrectos o incompletos, a través del uso no autorizado de datos o a través de intervención desautorizada en el proceso, será castigado con pena de privación de libertad de hasta cinco años o con multa.*

II. Procede aplicar el 263, apartados II a V.

El párrafo 263.a contempla la conceptuación de la figura como tipo básico en el inciso primero, y la sanción de la forma imperfecta de ejecución (tentativa) y un supuesto de agravación del tipo en razón de la gravedad del hecho (privación de libertad de uno a 10 años) por la remisión que efectúa al párrafo 263.

Se prescinde de la conceptuación restrictiva de los elementos clásicos de la estafa [70]que dificultan la aplicación de ésta a las defraudaciones cometidas mediante ordenador: el engaño a una persona (mención que no aparece en la estructura del tipo), el error en la misma (desaparece asimismo el requisito de provocación o mantenimiento del error en tercero), y el acto de disposición patrimonial lesivo (que en el caso de concurrir puede ser ya realizado tanto por una persona como por el propio ordenador automáticamente), requiriéndose en su lugar sólo al resultado de un perjuicio patrimonial para otro.

Permanecen los elementos subjetivos, especialmente el de la intención de conseguir una ventaja patrimonial, y los medios comisivos de influencia en el desarrollo del resultado de un proceso de transformación de datos se establecen alternativamente a través de la configuración errónea del programa, por medio del uso de datos incorrectos o incompletos, a través del uso no autorizado de datos o a través de intervención desautorizada en el proceso.

El proyecto del gobierno entendió por “proceso de datos” todos aquellos procesos técnicos en los que se alcanzan determinadas conclusiones de trabajo a partir de la toma de datos y de su puesta en relación según determinados programas. Se contempla aquí únicamente el proceso automático de datos. Según las reglas alemanas un programa es una instrucción completa para la resolución de una tarea junto con todos los ajustes precisos para ello, los programas informáticos son instrucciones de trabajo para el ordenador.

[70] El párrafo 263 I. Se refiere a la estafa en los siguientes términos “Quién, con la intención de procurar para sí o para un tercero una ventaja patrimonial ilícita, perjudique el patrimonio de otro causando un error o manteniéndolo, por medio de la apariencia de hechos falsos o de la desfiguración o supresión de hechos verdaderos, será castigado con pena de privación de libertad de hasta cinco años y con multa”.

La configuración incorrecta, es la modificación del programa para que sus instrucciones sean distintas a las concebidas inicialmente por su propietario: introducción de nuevas instrucciones o funciones en el programa, eliminación o alteración de su proceso de funcionamiento, modificación de los sistemas de control del propio programa, etc. El criterio para determinar la incorrección del programa es la intención del usuario del mismo, el hecho que éste lo haya aprobado por desconocimiento de la incorrecta configuración no exime de responsabilidad al sujeto activo del delito.

En cuanto a la situación que se refiere al empleo de datos incorrectos o incompletos comprende la manipulación en el *input* o entradas, no sólo por el operador o usuario del terminal que suministra de modo inmediato datos falsos a la instalación del proceso electrónico de datos, sino también por quienes los proporcionan de modo inmediato, como el personal de clasificación de datos (perforadores, mecanógrafos, etc.). Se incluyen los casos de determinación a través de terceros ajenos (ej. clasificación de datos primarios), como los casos de suministro inmediato, en que intercalan terceros que no practican ninguna comprobación material de los datos.

De acuerdo con la doctrina alemana, el que utiliza una tarjeta falsificada de acceso al ordenador emplea datos incorrectos del mismo modo de quien falsifica estados de cuenta. En cuanto a la influencia en el resultado de un proceso de elaboración de datos a través de un uso no autorizado de datos, la doctrina alemana, considera que de este modo se ha cubierto el supuesto del que mediante uso ilegítimo de tarjeta (las de cajero) y de códigos ajenos consiga acceder a sistemas informáticos con efectos patrimoniales de relevancia.

Respecto de la influencia en el resultado de un proceso de elaboración de datos a través de intervención no autorizada en el proceso, la misma doctrina, la

considera una fórmula amplia que pretende evitar posibles lagunas legales, abarcando supuestos no subsumibles en las alternativas anteriores, o de dudosa subsunción.

Ahora bien, al no recoger expresamente, la fórmula alemana, el término ordenador o informático tienen cabida en el precepto las manipulaciones fraudulentas de tipo patrimonial sobre cualquier tipo de sistemas automatizado de toma de decisiones, y no únicamente informático, consistiendo la acción típica en interferir en el resultado de un proceso de tratamiento de datos, de lo que se deriva una interferencia en una disposición patrimonial.

4.7.1.3. FALSIFICACIÓN DE DATOS PROBATORIOS.

Párrafo 269. *I. Quien, para engañar en el tráfico jurídico, almacene o altere datos probatorios relevantes de manera que en el momento de su recepción existiría un documento no auténtico o falsificado, o utilice datos almacenados o alterados de ese modo será castigado con pena de privación de libertad de hasta cinco años o con multa. II. La tentativa es punible. Deberá aplicarse el* P. *267, apartado III".*

La doctrina alemana, ha señalado que en ese país, el tipo de falsedad documental no es aplicable a la llamada falsificación de datos probatorios, debido a la imposibilidad de percibir directamente la declaración y la identidad del otorgante.

La acción consiste en modificar datos ya almacenados o almacenar otros nuevos con el mismo fin, o en utilizarlos en esas condiciones. Es necesario que la visualización de los datos sea equiparable a la existencia de un documento no auténtico o falsificado, es decir, que si fueran impresos o transcritos esos datos constituirían falsedad documental al tenor del párrafo 267.

En cuanto a los elementos del tipo subjetivo, además del dolo (basta que sea eventual), debe concurrir la intención de engañar en el tráfico jurídico. Según la doctrina alemana este requisito se cumple cuando el autor sólo quiere producir la manipulación en el proceso de datos, por lo tanto, no se exige el contacto personal entre el autor y la víctima (a diferencia de cómo es interpretado el engaño en el tipo de estafa). El artículo 270 aclara las dudas sobre el contenido de este elemento, con la innovación de equiparar el engaño a las manipulaciones informáticas, al disponer "*La falsificación de una elaboración de datos en el tráfico jurídico equivaldrá al engaño en el tráfico jurídico".* Esta norma es aplicable a todos los tipos legales en los que se exige "el engaño en el tráfico jurídico", teniendo gran importancia al considerar que la manipulación fraudulenta del proceso de datos produce un efecto similar al engaño.

4.7.1.4. ALTERACIÓN DE DATOS.

Párrafo 303.a. "*I. Quien borre, elimine, inutilice o altere ilícitamente datos (202.a, apartado II) será castigado con pena de privación de libertad de hasta dos años o con multa. II. La tentativa será punible".*

La disposición protege tanto al que almacena los datos, como a la persona afectada por el contenido de éstos. Objeto de la acción, son todos los datos no inmediatamente perceptibles en el sentido del párrafo 202.a.II. Se mencionan cuatro acciones típicas: a) el borrado, los hace desparecer de modo completo e irrecuperable (Ej. la destrucción de soportes, borrar los enlaces necesarios y perder la interpretabilidad, etc.); b) ocultar, privando del acceso a los mismos a la persona autorizada; c) inutilizar, cuando se dañan de manera tal que no puedan cumplir su fin; d) alterar, se trata de perturbaciones funcionales, como la transformación de su valor informativo, puede tener lugar a través del añadido

de datos, el borrado parcial o la puesta en relación con otros datos. Lo decisivo es que los datos posean un nuevo contenido una información alterada.

4.7.1.5. SABOTAJE INFORMÁTICO

Párrafo 303b. *"Quien destruya una elaboración de datos que sea de esencial importancia para una industria ajena, una empresa ajena o una autoridad,*
1. cometiendo el hecho de acuerdo al párrafo 303.a.II, o
2. destruyendo, dañando, inutilizando, eliminando o alterando una instalación de elaboración de datos o un soporte de datos, será castigado con pena de privación de libertad de hasta cinco años o con multa.
II. la tentativa será punible".
La finalidad perseguida por la legislación alemana, al crear el tipo de sabotaje informático diferenciado del tipo de alteración de datos, fue sancionar con mayor severidad las acciones que atentan contra procesos de datos que sean de importancia esencial para una empresa o establecimiento industrial ajenos o para la administración. Estas acciones pueden recaer en los equipos de procesamiento de datos, en los soportes y en los datos mismos. La doctrina entiende que es sancionado penalmente el que arremete a equipos o soportes de datos suyos en los que otras personas tengan un interés jurídicamente protegido o si borra datos que el mismo hubiera almacenado y que fueran procesados para terceros cuyo interés en su existencia se perjudica.

4.7.2. ESPAÑA

En España por otra parte, la solución fue dada Mediante Ley 10/95 donde se aprobó el Nuevo Código Penal español, entrando en vigor el 24 de mayo de 1996, ingresando a tipificar las conductas nocivas que se cometen a través de sistemas informáticos, Internet y adecuando aquellas conductas que se ven

facilitadas con los medios tecnológicos[71], inclusive creando un equipo policial especializado en la detección, represión de los delitos informáticos.

Dentro del capítulo X de los derechos contra la intimidad, el derecho a la propia imagen, y a la inviolabilidad del domicilio se encuentra el Art. 197.

1. El que para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, **mensajes de correo electrónico o cualesquiera otros documentos** o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

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

Con el fin de resguardar la intimidad de las personas sanciona la intrusión al correo electrónico protegiendo su contenido de la misma manera que las cartas

[71] Mediante sentencias de Tribunal Supremo de fechas 30-11-81; 29-11-84; 05-02-88; 15-02-90;30-11-92 Y otras, a través de la jurisprudencia vinculante se ha dado ingreso y validez al documento electrónico por vía analógica, otorgándole validez, siempre que sea autentico y haya sido obtenido lícitamente. Si bien es cierto que existan en la actualidad otros objetos que sin tener esa condición, puedan equiparse a los mismos

tradicionales y la interceptación de las telecomunicaciones, agravándolas si fueren difundidas o cedidas a terceros, asimismo si el autor fuera responsable de los registros o archivos, refrendando su posición en relación al documento electrónico que por analogía fue objeto de protección.

Dentro el capítulo de las defraudaciones está incluida la estafa en el Art. 248

1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.

2. También se consideran reos de estafa los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero.

En materia de estafas electrónicas los legisladores españoles sin ingresar a mayores discusiones incorporaron un tipo penal de estafa que acoge la particularidad de la transferencia del activo patrimonial mediante manipulación informática o artificio semejante, ya sea por modificaciones de programas o alteraciones en el procesamiento, suprimiendo lo relacionado al engaño, artificios, elemento que fue discutida en lo relacionado al engaño a una maquina, suprimiendo el principal obstáculo al adecuarla a la estafa facilitada por un computador, en cuanto a su sanción se toma en cuenta el importe de lo defraudado, las relaciones existentes entre autor y víctima, los medios empleados.

Con referencia al sabotaje informático tenemos el **Artículo 264.** (En su numeral 2)

2. La misma pena se impondrá al que por cualquier otro medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

Establece una sanción de uno a tres años de prisión y multa de doce a veinticuatro meses, así el delito de sabotaje informático se equipara al tipo penal de daños protegiendo los programas, archivos y ficheros económicamente evaluables para la actividad empresarial, toda vez que la información personal es objeto de protección en el Art. 197.

En relación al espionaje informático se tipifica en el Art. 278

1. El que, para descubrir un secreto de empresa se apodere por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieren al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.
2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Como aquella conducta nociva con la finalidad de obtener datos almacenados en un soporte informático por cualquier medio, caracterizado por su valor económico, confidencialidad y exclusividad.

4.7.3. FRANCIA

Con la Ley de Modificación del Código Penal, número 88-19, de 5 de enero de 1988, relativa al fraude informático, también conocida como "*loi Godfrain*", el legislador recogió en un nuevo Capítulo del Código Penal, bajo la rúbrica "Sobre ciertas infracciones en materia informática" (especialmente los delitos vinculados a la piratería, intrusión, traba al funcionamiento, esto es virus y ciertas asociaciones que pueden ser de hackers) toda la nueva realidad criminal compleja vinculada a las nuevas tecnologías de la información, pero siempre y cuando no tuvieran ya una adecuada inclusión bajo figuras clásicas existentes. En este sentido, la utilización frecuente del término "informatisé" (informatizado) sobre el de "informatique" (informático), ha hecho pensar a la doctrina que el legislador se ha preocupado de proteger la información en su conjunto y no sólo aquella en soporte informático, es decir, que su preocupación se ha centrado en las conductas fraudulentas de acceso y uso ilícito de los sistemas de tratamiento automatizado de datos, absteniéndose de regular las manipulaciones informáticas con ánimo de lucro y en perjuicio patrimonial de tercero, núcleo principal del fraude informático.

Es así como, el título genérico de la ley hace referencia al fraude informático, en el enunciado, en su texto no aparece ninguna referencia específica al mismo. Es más, la ley sanciona específicamente la falsedad informática, sólo cuando el dato alterado se encuentre sobre un soporte informático.

Por lo tanto, las defraudaciones patrimoniales por medios informáticos quedan sin regulación especial, porque de acuerdo con las decisiones y jurisprudencia de la Corte de Casación Francesa y de los Tribunales de Apelación, aquellas venían siempre subsumidas en la figura clásica de estafa del Art. 405 del Código Penal, que sanciona al que "*haciendo uso de falsos nombres o de falsas cualidades, bien empleando maniobras fraudulentas para simular la existencia*

de falsas empresas, de un poder o crédito imaginario, o por hacer nacer la esperanza o la creencia de un suceso, de un accidente o de cualquier otro acontecimiento imaginario, se haya hecho reintegrar o traspasar, o hubiera intentado hacerse reintegrar o traspasar fondos, muebles, obligaciones, disposiciones, billetes, promesas, deducciones o desgravaciones, y hubiera por uno de estos medios, defraudado o intentado defraudar la totalidad o parte de la fortuna de otro".

La subsunción es posible al recogerse en la descripción de la conducta típica la cláusula "maniobras fraudulentas" y el "perjuicio", debiéndose entender éstas como formas de engaño, siendo las manipulaciones informáticas integrables en aquéllas, y la omisión del texto a referencias genéricas sobre el "engaño", el "error" y al "acto de disposición". Al respecto, según la doctrina, la ley de reforma francesa se concibe materialmente como una vía para reprimir accesos abusivos a los sistemas informáticos y actuaciones ilícitas sobre datos informatizados y su tratamiento, se produzca o no perjuicio, habiéndose rechazado de forma expresa en el proceso de tramitación parlamentaria las propuestas de subsumir las agresiones patrimoniales por medios informáticos en los tipos recogidos por esta ley.

La reforma penal de 1992, Ley 92-683, vigente a partir de marzo de 1994, introdujo cambios en el texto legal de las disposiciones informáticas y las trasladó a otra parte del Código, esto es, al Libro III, Título II, Capítulo III: De los atentados contra los sistemas de tratamiento automatizado de datos. La falsificación informática que estaba regulada en los artículos 462-5 y 462-6, sobre la falsificación y uso de documentos electrónicos falsificados, actualmente en el nuevo Art. 441-1, que se refiere a todas las posibles formas de un documento, incluyendo el electrónico. El acceso fraudulento en sistemas informáticos en el actual 323-1, sabotaje informático en el artículo 323-2.

4.7.3.1. Acceso fraudulento a un sistema de elaboración de datos.

Artículo 323-1. "*El hecho de acceder en forma fraudulenta a la totalidad o parte de un sistema de tratamiento automatizado de datos, o de mantenerse en él, será castigado con un año de prisión y multa de 15.000 euros. Si de ello resultare, bien la supresión o la modificación de datos contenidos en el sistema, o una alteración del funcionamiento de este sistema, la pena será de dos años de prisión y de 30.000 euros de multa".*

Para que se entienda consumado este delito, no se requiere la alteración, daño o destrucción de los datos contenidos en el sistema, ni el apoderamiento, uso o conocimiento de la información contenida en él, y tampoco la revelación o difusión de los datos contenidos en ese sistema. La mención a "mantenerse en él", se refiere al acceso que ocurre en forma accidental o casual.

4.7.3.2. Sabotaje informático

Artículo 323-2. *"El hecho de obstaculizar o alterar el funcionamiento de un sistema de tratamiento automatizado de datos será castigado con tres años de prisión y multa de 45.000 euros".*

La legislación francesa, al igual que la alemana distingue entre el delito de sabotaje informático y la alteración de datos.

4.7.3.3. Destrucción de datos.

Artículo 323-3. *"El hecho de introducir de manera fraudulenta datos en un sistema de tratamiento automatizado o de suprimir o modificar fraudulentamente los datos que contengan será castigado con tres años de prisión y multa de 45.000 euros".*

El objeto del delito son los datos contenidos en un sistema de tratamiento de los mismos.

4.7.3.4. Asociaciones para cometer delitos informáticos[72].

Artículo 323-4. *"La participación en un grupo formado o en un acuerdo establecido para la preparación, caracterizada por uno o varios hechos materiales, de una o varias de las infracciones previstas en los artículos 323-1 a 323-3 será castigada con las penas previstas para la misma infracción o para la infracción castigada más severamente".* Se trata de los llamados Clubs de Hackers.

Artículo 323-5. *"Las personas físicas culpables de los delitos previstos en el presente capítulo incurrirán igualmente en las penas accesorias siguientes:*

1º La prohibición, por un período hasta de cinco años, del ejercicio de derechos cívicos, civiles y de familia, según las modalidades del artículo 131-26;

2º La prohibición, por un período de hasta cinco años, de ejercer una función pública o de ejercer la actividad profesional o social en el ejercicio de la cual o con ocasión de la cual se haya cometido la infracción;

3º El comiso de la cosa que haya servido o estaba destinada a cometer la infracción o de la cosa producto de la misma, con excepción de los objetos susceptibles de restitución;

---

[72] La Organización transnacional Business software Alliance, reporto el 4 de agosto del 2010, que habla recibido 15'840 denuncias sobre piratería de software de las cuales resultaron 15'714 acciones legales en toda Europa.

4º La clausura, por un período de hasta cinco años, de los establecimientos o de uno o varios de los establecimientos de la empresa que hayan servido para cometer los hechos incriminados;

5º La exclusión, por un período de hasta cinco años de los contratos públicos;

6º La prohibición, por un período de hasta cinco años, de emitir cheques, salvo los que permitan la retirada de fondos por el librador contra el librado o los que estén conformados;

7º La publicación o la difusión de la resolución adoptada en las condiciones previstas en el artículo 131-35".

Artículo 323-6. *"Las personas jurídicas podrán ser declaradas penalmente responsables de las infracciones definidas en el presente capítulo en las condiciones previstas en el artículo 121-2.*
Las penas aplicables a las personas jurídicas serán:

1º La multa, conforme a lo previsto en el artículo 131-38;

2º Las penas mencionadas en el artículo 131-39.

La prohibición mencionadas en el apartado 2º del artículo 131-39 se aplicará a la actividad en cuyo ejercicio o con ocasión de la cual se haya cometido la infracción".

Artículo 323-7. *"La tentativa de los delitos previstos en los artículos 323-1 a 323-3 será castigada con las mismas penas".*

4.7.3.5. Falsificación y uso de documentos electrónicos falsificados.

Artículo 441-1. *"Constituye una falsedad toda alteración fraudulenta de la verdad, susceptible de causar un perjuicio y realizada por cualquier medio, en un escrito o en cualquier otro medio de expresión de pensamiento que tenga por objeto o que pueda tener como efecto constituir la prueba de un hecho con consecuencias jurídicas o de un derecho".*

El legislador francés suprimió los artículos 462-5 y 462-6, sobre falsificación y uso de documento electrónico falsificado, y amplió el concepto de documento de manera de incluir los electrónicos.

4.7.4. ESTADOS UNIDOS

En 1994 Estados Unidos adoptó el Acta Federal de Abuso Computacional (18 U.S.C. Sec.1030) que modificó al Acta de Fraude y Abuso Computacional de 1986. Con la finalidad de eliminar los argumentos híper técnicos acerca de qué es y qué no es un virus, un gusano, un caballo de Troya, etc., y en qué difieren de los virus, la nueva ley sanciona la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas (18 U.S.C.: Sec. 1030(a)(5)(A)). La nueva ley es un adelanto porque está directamente en contra de los actos de transmisión de virus.

El Acta de 1994 diferencia el tratamiento sobre los autores de los virus con intención de causar daños y estragos de aquellos imprudentes creadores que por su negligencia lanzan un virus, estableciendo para los primeros una pena de hasta diez años en prisión federal más una multa y para los segundos la sanción fluctúa entre una multa y un año en prisión. Aclarando que el creador de un virus no podrá escudarse en el hecho de que no conocía que con su actuar causaría daño a alguien o que él solo quería enviar un mensaje. Con

esta inclusión se elimina la concepción de que el sujeto activo debía poseer conocimientos superiores para la realización de estos actos.

En opinión de los legisladores esta nueva ley es más flexible en el sentido de que debido al incremento de los delitos informáticos y las distintas formas de ataque tecnológico que sufren las empresas, la NASA, el Pentágono inclusive la Casa Blanca, etc., violando los mecanismos de seguridad informática, no se enfrascan en una definición de los virus sino por el contrario describen el acto como instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar o transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas, para que pueda dar cabida en un futuro a la nueva era de ataques tecnológicos.

En materia de estafas electrónicas, defraudaciones y otros actos dolosos relacionados con los dispositivos de acceso a sistemas informáticos, se sanciona con pena de prisión y multa, a la persona que defraude a otro mediante la utilización de una computadora o red informática.

La ley de privacidad adoptada por el Estado de California en 1992 contempla delitos informáticos en menor grado que los delitos relacionados con la intimidad, sin embargo es importante destacar las enmiendas realizadas a la Sección 502 del Código Penal ampliándose los sujetos susceptibles de verse afectados por estos delitos aumentando de esta manera la protección a individuos, negocios, agencias gubernamentales y otros, de la interferencia, del daño y acceso no autorizado a las bases de datos, la creación de sanciones pecuniarias de diez mil dólares por cada persona afectada y hasta cincuenta mil dólares el acceso imprudencial a una base de datos, todo ello a raíz del desarrollo tecnológico.

El Instituto de Seguridad Informática (CSI Computer Security Institute)[73] señala que los tipos de delitos y pérdidas de datos informáticos son a consecuencia de errores humanos, problemas de seguridad y otros.

4.7.5. CHILE

Chile fue el primer país Latinoamericano en sancionar una Ley Contra Delitos Informáticos (Ley No. 19223), fue promulgada el 28 de mayo de 1993, y entró en vigencia el 7 de junio de 1993, esta ley tiene antecedentes en la legislación francesa que data de 1988, contiene solamente 4 artículos referidos exclusivamente a ciertos actos constitutivos de delito informático.

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

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicará la pena señalada en el inciso anterior, en su grado máximo.

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

[73] En http://delitosinformaticos.com

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

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

Según esta ley, en su Art. 1 Podemos decir que el legislador chileno tiende a proteger el software como el hardware del computador, asimismo establece que el actor debe actuar con dolo, es decir que su conducta debe ser intencional, que al tener los conocimientos necesarios comprende su accionar, estableciéndose entonces que no se sanciona la conducta culposa.

En el Art. 2 tipifica el intrusismo que tiene la finalidad de apoderarse, usar o conocer indebidamente la información, poniendo en relieve el aspecto subjetivo "animo".

El Art. 3 En este caso sanciona el daño causado a la información contenida en un sistema informático, dolosamente.

Finalmente el Art. 4 se refiere a la divulgación maliciosamente de datos contenidos en un sistema de información, agravándose la pena si fuere el responsable del sistema de información.

4.7.6. PERU

El Gobierno Peruano incorpora los delitos informáticos en su legislación mediante Ley No 27309, que modifica el Título V, Capitulo X del Libro Segundo

del Código Penal, incorporando el Capítulo X titulado Delitos Informáticos de la siguiente manera.

Art.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 ó copiar información en tránsito 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 cincuentaidós a ciento cuatro jornadas.

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

En este artículo el legislador peruano sanciona la utilización e ingreso indebido a una base de datos (delito de peligro), pero con la misma sanción se tipifica las conductas de interferir, acceder o copiar información (delito de resultado), en su parágrafo segundo se encuentra la agravante cuando el autor obtiene un beneficio económico, se puede observar que en un artículo vinculan los bienes jurídicos de la intimidad con el patrimonio.

Art.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 con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

En este Artículo se tipifica la figura del sabotaje informático, que tiene como objetivo la lesión al patrimonio representado por los sistemas informáticos y programas de computadoras del sujeto pasivo.

Art. 2O7 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.

Las agravantes se dan cuando el sujeto activo se aprovecha de su cargo para obtener información o en su caso la puesta en peligro la seguridad nacional de Perú.

4.7.8. ECUADOR

La vocación del delito de estafa en el Ecuador para asumir las diferentes modalidades del fraude informático deriva en una atipicidad relativa si cabe el término, ya que tanto sus elementos objetivos como subjetivos no encuentran fundamento (a excepción del ánimo de apropiación) dentro del llamado Fraude Informático, ya que serían tipos completamente diferentes, así que en aplicación del principio de legalidad, el tipo penal de estafa no podría ser aplicado al fraude informático en razón de que sus elementos subjetivos y objetivos tienen connotaciones distintas, lo que torna en inaplicable a dicho tipo penal clásico.

4.7.9. ARGENTINA

El 04 de Junio de 2008, fue sancionada la Ley 26.388 de Delitos Informáticos, incorporándose así Argentina a la lista de países que cuentan con regulación legal sobre esta importante cuestión.

La Ley 26.388 no es una ley especial, que regula este tipo de delitos en un cuerpo normativo separado del Código Penal (CP) con figuras propias y específicas, sino una ley que modifica, sustituye e incorpora figuras típicas a diversos artículos del CP actualmente en vigencia, con el objeto de regular las nuevas tecnologías como medios de comisión de delitos previstos en el CP.
Delitos informáticos penados y penas instituidas, a lo largo de su articulado tipifica, entre otros, los siguientes delitos informáticos:

- Pornografía infantil por Internet u otros medios electrónicos (art. 128 CP);

- Violación, apoderamiento y desvío de comunicación electrónica (art. 153, párrafo 1º CP);

- Intercepción o captación de comunicaciones electrónicas o telecomunicaciones (art. 153, párrafo 2º CP);

- Acceso a un sistema o dato informático (artículo 153 bis CP);

- Publicación de una comunicación electrónica (artículo 155 CP);

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

- Revelación de información registrada en un banco de datos personales (artículo 157 bis, párrafo 2º CP);

- Inserción de datos falsos en un archivo de datos personales (artículo

157 bis, párrafo 2º CP; anteriormente regulado en el artículo 117 bis, párrafo 1º, incorporado por la Ley de Hábeas Data);

- FRAUDE INFORMÁTICO (artículo 173, inciso 16 CP);

- Daño o sabotaje informático (artículos 183 y 184, incisos 5º y 6º CP).

Las penas establecidas son: a) prisión; b) inhabilitación (cuando el delito lo comete un funcionario público o el depositario de objetos destinados a servir de prueba); c) multa.

CAPITULO V
MARCO PRÁCTICO

5.1. BALANCE ESTADISTICO DE LOS CASOS REGISTRADOS EN DIFERENTES INSTITUCIONES DE JUSTICIA.

El trabajo de campo realizado y los resultados obtenidos se constituyen en la base empírica para justificar la evaluación del problema de del vacío legal que existe en nuestra legislación penal conforme al Fraude Informático.

5.1.1. Casos registrados en los Tribunales sobre Delitos de Estafa y Manipulación Informática, combinados en uno solo.

Tabla 1:

LUGAR	GESTION 2010	GESTION 2011
JUZGADO DE INSTRUCCIÓN EN LO PENAL	9	11
JUZGADO DE PARTIDO EN LO PENAL	0	0
TRIBUNALES DE SENTENCIA	0	0
TOTAL	9	11

Fuente: Tribunal Departamental de Justicia de La Paz

De los datos registrados se observa un incremento de 2 casos en el 2011 en los Juzgados de Instrucción en lo Penal, y ni un solo caso registrado en los Juzgados de Partido ni los Tribunales de Sentencia, esto demuestra que si bien existen este tipo de denuncias, estas no tienen un avance significativo ya que según las entrevistas que se realizaron, suceden dos casos: o bien la parte denunciante abandona el caso por poder aportar pruebas suficientes o se complica la investigación de la misma, esto se debe a que el IDIF (Instituto de Investigaciones Forenses) no cuenta con ningún perito en esta área, por lo que muchas veces la parte denunciante debe proporcionar el perito y pagar por sus pericias que según se dice son las pericias más caras del país.

5.1.2. Casos registrados en los Juzgados de Instrucción sobre delitos informáticos.

Tabla 2:

GESTION	MANIPULACION INFORMATICA	MANIPULACION INFORMATICA	ALTERACION, ACCESO Y USO

	CON ESTAFA Art. 363 Bis. y Art. 335 del C.P.	Art. 363 Bis. Del C.P.	INDEBIDO DE DATOS INFORMATICOS Art. 363 Ter.
2010	9	4	0
2011	11	6	0
TOTAL	20	10	0

Fuente: Tribunal Departamental de Justicia de La Paz

De los datos recolectados se evidencia que el Fraude Informático lleva un rango mayor de denuncias frente a los otros delitos informáticos tipificados en nuestro Código penal, la Manipulación lleva el segundo lugar con el 50% de los Fraudes Informáticos y la Alteración acceso y uso indebido no tiene denuncias, lo cual nos lleva a demostrar la hipótesis planteada para el presente tema de investigación.

5.1.3. Casos registrados en la Fiscalía, División de Economicos y Financieros

Tabla 3:

GESTION	MANIPULACION INFORMATICA CON ESTAFA Art. 363 Bis. y Art. 335 del C.P.	MANIPULACION INFORMATICA Art. 363 Bis. Del C.P.	ALTERACION, ACCESO Y USO INDEBIDO DE DATOS INFORMATICOS Art. 363 Ter.	TOTAL
2010	11	4	0	15

2011	15	6	0	21
TOTALES	26	10	0	36

Fuente: Fiscalía de Distrito

Del total de los casos registrados, se observa que si bien existen denuncias de Fraude Informático, estas son subsumidas en dos tipos penales diferentes como la Estafa y la Manipulación Informática, y según nos informa el Fiscal de Materia de la División de Economicos y Financieros, que este tipo de casos son muy complicados, primero porque se hace muy difícil encuadrar estos dos delitos en un mismo hecho y segundo que en el IDIF no existe un perito de esta naturaleza, entonces las partes deben proporcionar el perito adecuado lo que les cuesta mucho dinero y mucho tiempo por lo cual algunas de estas denuncias se traban en la Etapa Preliminar, sin embargo hacemos todo lo que está a nuestro alcance para proseguir con las investigaciones, actualmente tenemos 2 detenidos por Estafa y Manipulación Informática que son los casos de Banco Bisa y COMPANEX Ltda.

Para corroborar lo mencionado por el Sr. Fiscal, debemos realizar una comparación entre la Tabla 1 y la Tabla 3 (Ver tabla 1 y 3), y veremos que en el 2010 solo 9 de 11 casos ingresaron a los Juzgados de Instrucción y en el 2011 solo 11 de 15 casos hicieron lo mismo.

5.1.4. Denuncias registradas en la FELCC La Paz, División Economicos y Financieros

Tabla 4

GESTION	MANIPULACION	MANIPULACION	ALTERACION,

	INFORMATICA CON ESTAFA Art. 363 Bis. y Art. 335 del C.P.	INFORMATICA Art. 363 Bis. Del C.P.	ACCESO Y USO INDEBIDO DE DATOS INFORMATICOS Art. 363 Ter.
2010	25	13	3
2011	21	26	5
TOTAL	46	39	8

Fuente: FELCC La Paz.

Los datos obtenidos muestran que las denuncias de este tipo recaen en mayor número en la FELCC, tomando en cuenta que las tablas anteriores no tenían porcentajes como esta, sin embargo vemos que el fraude Informático sigue siendo el más denunciado.

En la entrevista realizada al Teniente Elviz Núñez Fernández, el cual es el único investigador de la División de Economicos Financieros de la FELCC, nos dice que las denuncias sobre Delitos Informáticos llegan a sus manos y con respecto al tema de la investigación nos dice que sería muy bueno que se tipifique el fraude Informático, ya que de esa manera el trabajo se le haría más cómodo y sería beneficioso para las personas que denuncian este tipo de casos, entre otras cosas nos informa que si bien estas denuncias no llegan a la querella correspondiente ante el Ministerio Publico en muchos casos es porque nosotros informamos a las partes que el IDIF no cuenta con un perito en Informática y por lo tanto la parte interesada debe proporcionar este que es muy costoso y demoroso.

Además nos informa que la Policía Boliviana si cuenta con un perito en Informática Forense, el cual es el Capitán Llanos que trabaja en la ANAPOL

Seguencoma pero aun no esta autorizado a realizar peritajes, puesto que su función será a partir de la promulgación de la nueva Ley del Ministerio Publico.

5.2. BALANCE REGISTRADO DE LAS ENCUESTAS REALIZADAS A PERSONAS NATURALES.

Las Encuestas realizadas nos arroja datos sobre la situación real de las personas que necesitan del mundo del internet para realizar sus actividades día a día.

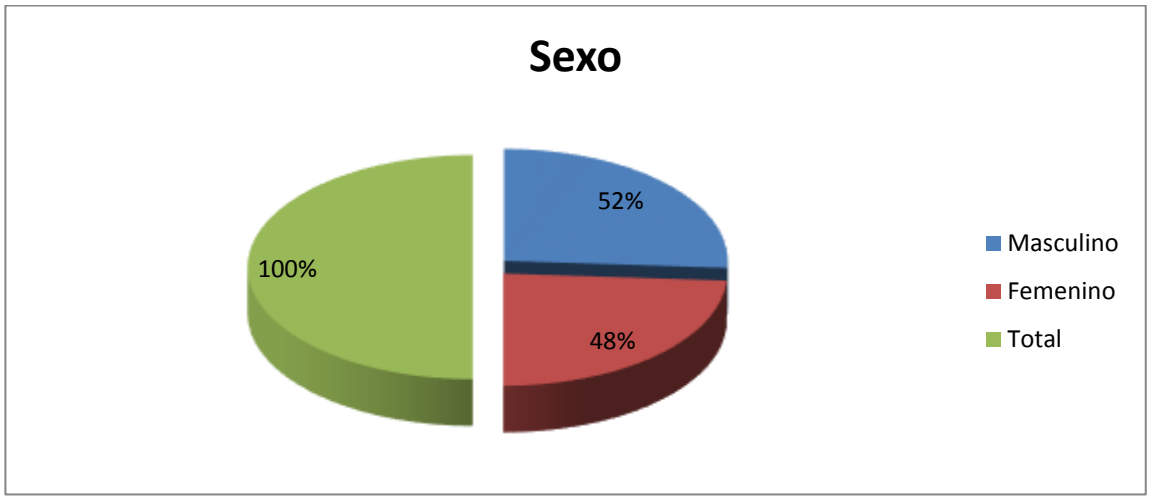
En cuanto a las encuestas estas fueron dirigidas en forma proporcional tanto a personas que realizan distintas actividades en un café Internet, como a personas clientes de entidades Financieras.

5.2.1. PROMEDIO DE GÉNERO ENTRE LAS PERSONAS ENCUESTADAS

A manera de igualdad de género y equidad, las encuestas se dividieron en forma proporcional, entre hombres y mujeres, demostrando que tanto hombres y mujeres transitan por el mundo cibernético y como alguno de ellos mención que son llamados Cibernautas.

Grafico Nº 1

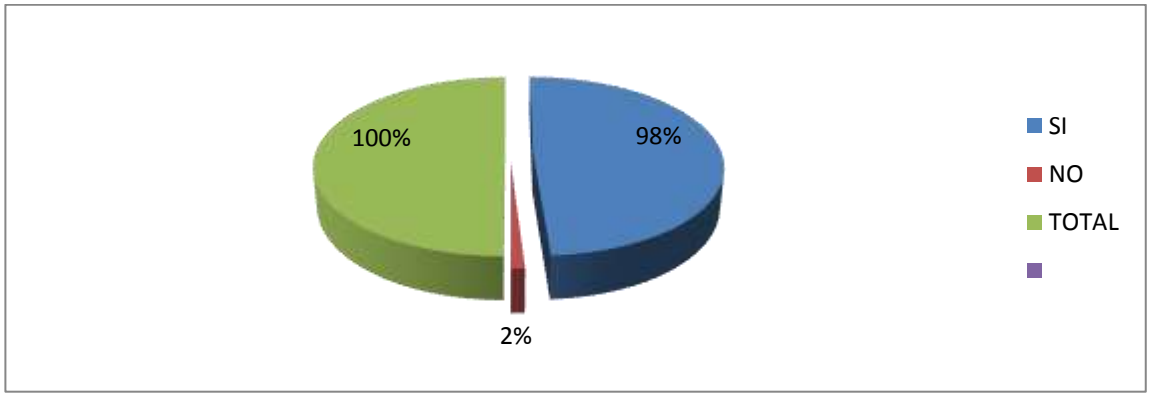
Sexo



Fuente: Elaboración Propia[74]

5.2.2. USTED TIENE UN SITIO EN LA RED COMO SER CORREO ELECTRONICO, FACEBOOK, EMAIL, ETC.

Grafico Nº 2



Fuente: Elaboración Propia[75]

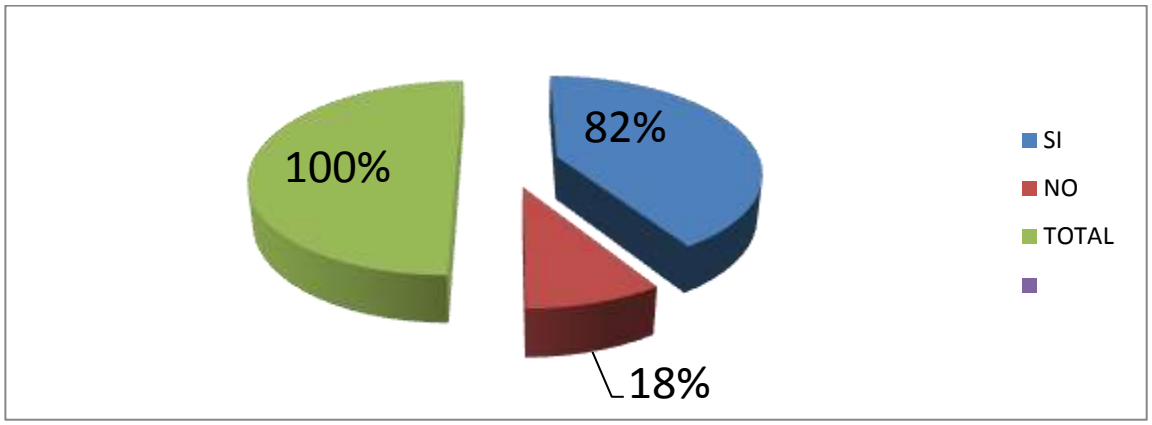
Definitivamente como ya lo habíamos mencionado, la equidad de género hoy en día está presente en casi todos los ámbitos de nuestra sociedad, pues así lo

[74] Fuente Propia
[75] Fuente Propia

demuestra el grafico 2, que tanto mujeres y varones si tienen un sitio en la red sea cual sea este.

5.2.3. USTED ES CLIENTE DE ALGUN BANCO

Grafico Nº 3



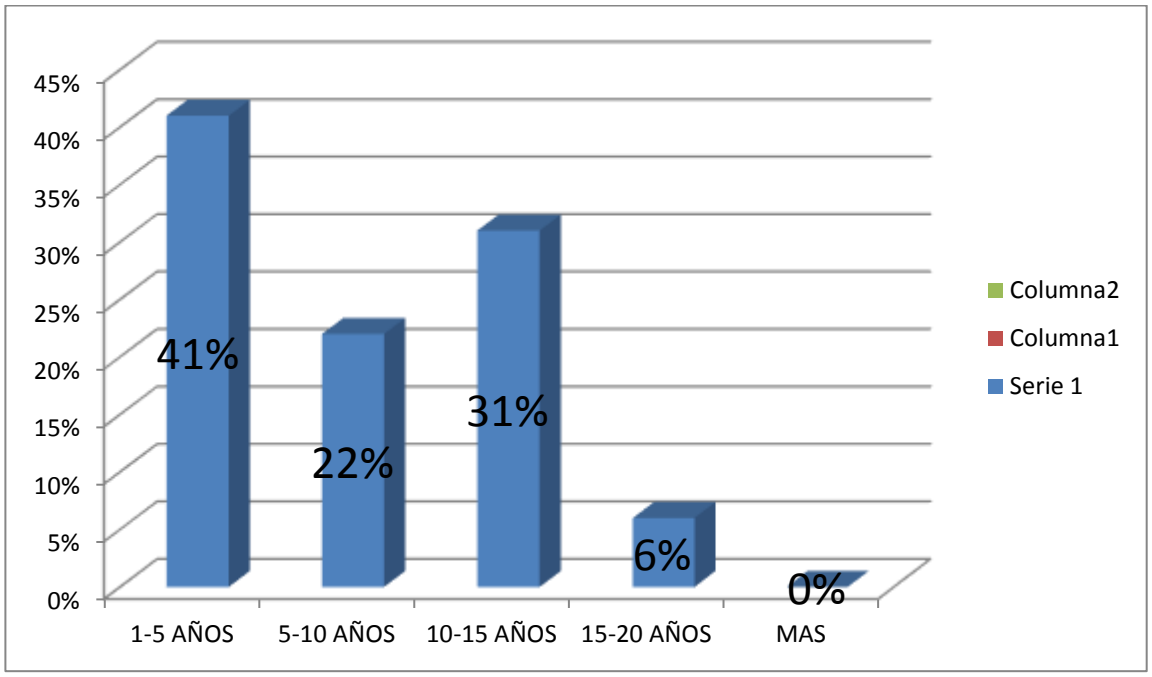
Fuente: Elaboración Propia[76]

En este grafico, nos da a conocer que la gran mayoría de los encuestados son actualmente clientes de una entidad financiera y un porcentaje menor indica que no tienen relación, por lo cual demuestra que si bien estos dos grupos tienen un espacio en la red, solo el 82% son clientes de un banco.

5.2.4. SI RESPONDIO AFIRMATIVAMENTE LA PREGUNTA ANTERIOR, CUANTOS AÑOS LLEVA DE SER CLIENTE DE SU BANCO

Grafico Nº 4

[76] Fuente Propia



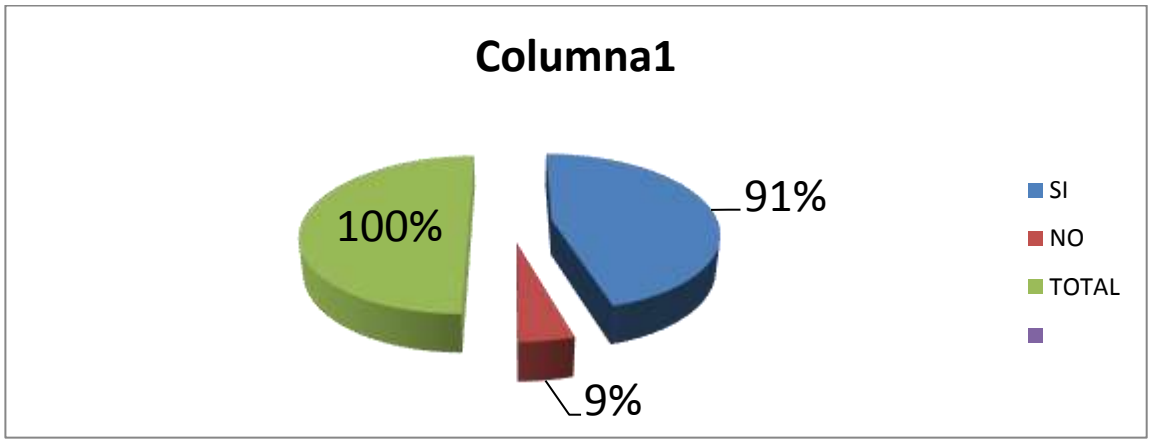
Fuente: Elaboración Propia[77]

El grafico nos muestra que la gente encuestada en relación a la antigüedad que tiene como cliente de su banco está por decir en término medio ya que los que recién tienen entre 1 a 5 años de cliente superan a todos pero en segundo lugar están los clientes de 10 a 15 años, es decir se nota que hay una confianza y fidelidad en su banco.

5.2.5. ALGUNA VEZ USTED HA SUFRIDO EL ACCESO NO PERMITIDO EN SU ESPACION EN LA RED. CORREO, E-MAIL, FACEBOOK, CUENTA BANCARIA, ETC.

Grafico Nº 5

[77] Fuente Propia

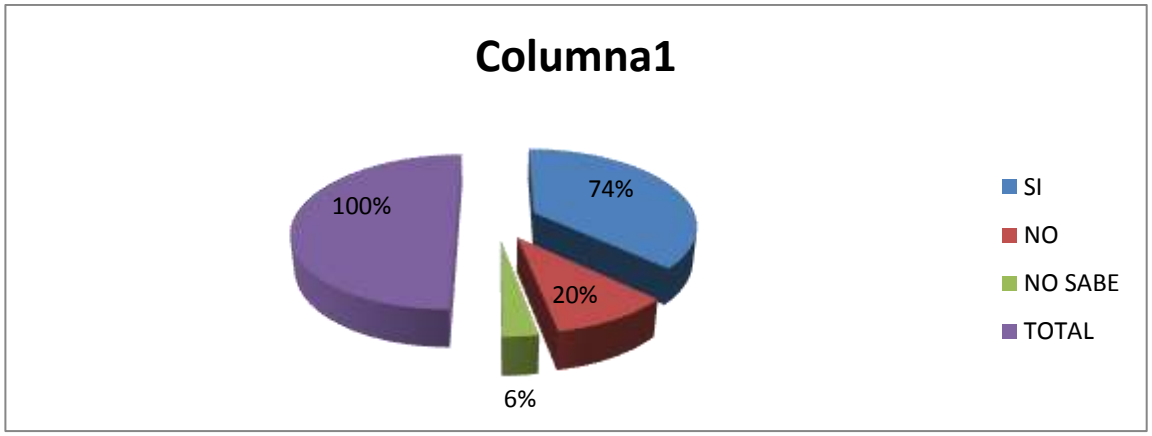


Fuente: Elaboración Propia[78]

El grafico muestra que la mayoría de los encuestados si sufrieron alguna vez un acceso en su espacio en la red.

5.2.6. USTED HA SIDO VICTIMA DE ALGUN DELITO INFORMATICO

Grafico Nº 6



Fuente: Elaboración Propia[79]

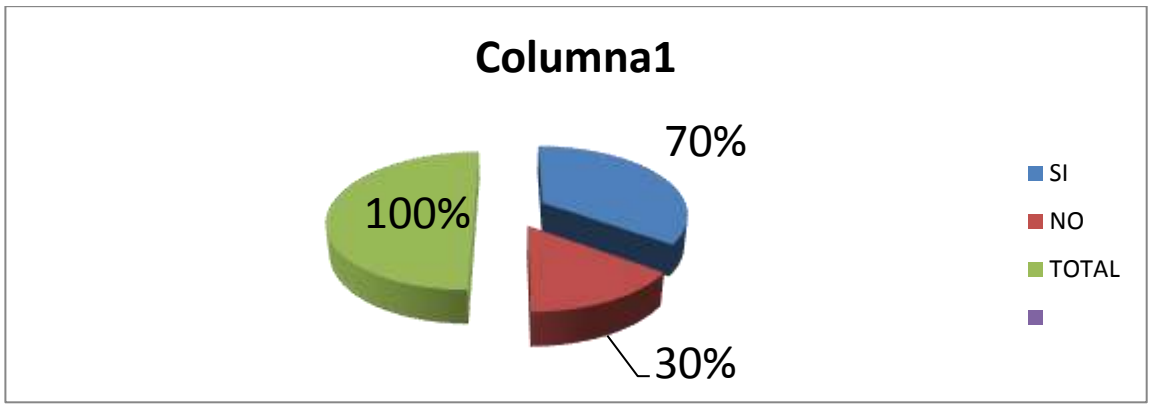
Como vemos en el grafico el 74% de los encuestados si han sido víctimas de algún delito informático, entonces si hacemos una comparación con el grafico Nº 5, supondríamos que el 17% que respondió que sí tuvo acceso no permitido

[78] Fuente Propia
[79] Fuente Propia

en su sitio en la Red fueron víctimas de algún hacker sin malas intenciones, y nada mas descifraron sus contraseñas de acceso.

5.2.7. SABE LO QUE ES EL FRAUDE INFORMATICO O ESTAFA A TRAVES DEL INTERNET

Grafico Nº 7



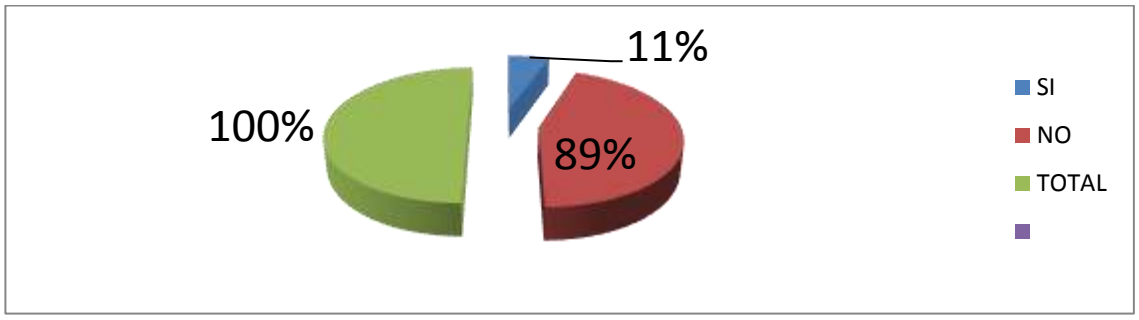
Fuente: Elaboración Propia[80]

El grafico nos arroja datos que son relevantes para la presente investigación, ya que el 70% de los encuestados si sabe lo que es un fraude Informático y el otro 30% no, lo que indica que si bien este delito no está tipificado en nuestro Código penal, la gente ya ha oído hablar de él y sabe cómo se realiza.

5.2.8. AL HABER SIDO VICTIMA DE UN FRAUDE INFORMATICO USTED HIZO LA DENUNCIA

Grafico Nº 8

[80] Fuente Propia



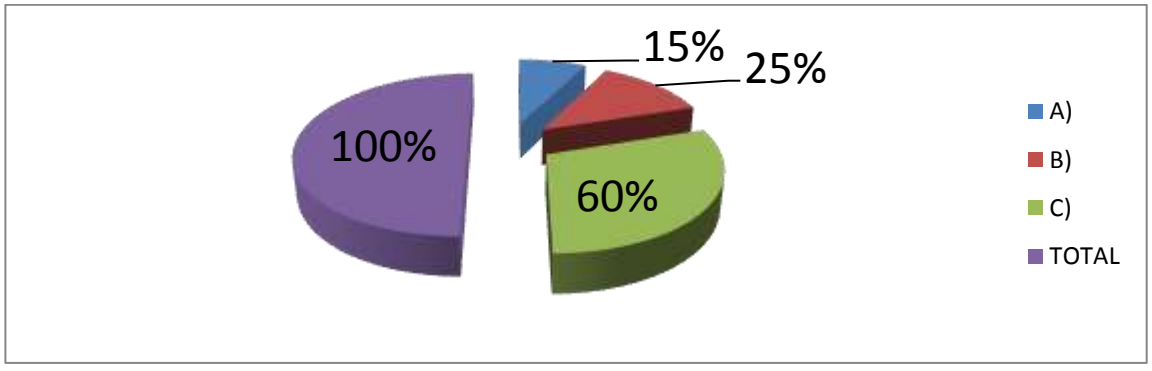
Fuente: Elaboración Propia[81]

En el grafico se muestra un detalle muy significativo para la presente investigación ya que al parecer, realizando una mirada al grafico 6 se demuestra que el 74% de los encuestados si han sufrido algún delito informático pero solo el 11% lo denuncio, pero la causa la conoceremos con el siguiente grafico.

5.2.9. EN CASO DE NO HABER REALIZADO LA DENUNCIA, NI SEGUIR EL PROCESO PENAL CORRESPONDIENTE, ES A CAUSA DE:

A) FACTOR TIEMPO
B) LAS PENAS SON MUY BAJAS A COMPARACION DEL COSTO DEL PROCESO
C) DESCONOCE EL LUGAR DONDE SE REALIZA LA DENUNCIA

Grafico Nº 9

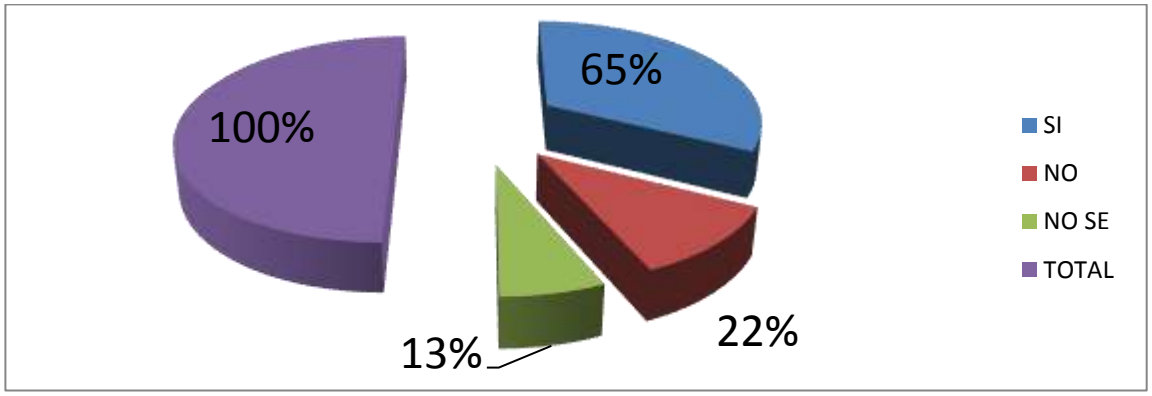


[81] Fuente Propia

Fuente: Elaboración propia[82]

5.2.10. USTED ESTARIA DE ACUERDO QUE SE INCORPORE EL FRAUDE INFORMATICO EN EL CODIGO PENAL COMO NUEVO DELITO

Grafico Nº 10



Fuente: Elaboración propia[83]

Como se puede observar la mayor parte de los encuestados, que repetimos, son personas que diariamente utilizan sus espacios en la red, opina que es necesario que se regule el Fraude Informático, entonces de esa manera alivianar el trabajo tanto de abogados, fiscales, jueces, peritos, y todo aquel que tenga que ver, para poder administrar justicia correctamente y así castigar a aquellos delincuentes que operan a través de las redes sin ser vistos ni oídos quedando impunes a la justicia y la sociedad.

5.3. CONCLUSIONES DEL MARCO PRÁCTICO

- Analizando los datos obtenidos tanto en las entrevistas como en las encuestas realizadas, establecemos que se requiere con

[82] Fuente Propia
[83] Fuente Propia

urgencia la incorporación el Fraude Informático al Código Penal Boliviano como un nuevo delito a causa de la tecnología.

- Es necesario la modernización e incorporación de políticas referentes a los delitos Informáticos, en cuanto a la protección de los datos vertidos a través de medios informáticos, a fin de garantizar seguridad a la población que necesariamente tiene un espacio en la red.

- Es imprescindible la pronta elaboración de una Ley Especial que luche contra estas nuevas formas de delinquir.

- Es importante valorizar las pérdidas económicas que sufre una víctima de fraude informático, tomando en cuenta que estas podrían ser millonarias y la pena podría ser insignificante, evitando siempre que se vulneren los derechos del individuo ya que como investigamos los peritajes no salen nada baratos.

- Para tener un debido proceso, con pruebas fehacientes en la fase investigativa de la etapa preliminar o preparatoria, que es donde a menudo se estanca este tipo de procesos, se deberá impartir enseñanza y capacitación a efectivo policiales que cumplen con la labor investigativa, a través de cursos o seminarios, para que los mismos tengan conocimiento adecuado cuando se presente alguna denuncia de esta naturaleza.

- Se deberá contar con personal altamente calificado y crear una división especial en el Ministerio publico para encargarse

solamente de delitos informáticos, como el ejemplo que nos dio el Ing. Oscar Guzmán Jordán, Administrador de Red de la Carrera de Informática de la UMSA, en la entrevista que le hicimos, donde nos indico que la carrera está trabajando en una propuesta sobre la creación de la división de Delitos Informáticos, que estaría compuesta por Ingenieros de Sistemas que se ocupen de rastrear delitos informáticos en las redes pero siempre bajo la dependencia de un fiscal especialista en este tipo de delitos.

5.4. COMPROBACION DE LA HIPOTESIS

En la investigación de la presente tesis se llega a establecer la hipótesis respecto a: “La tipificación del "Fraude informático" en el código penal boliviano, permitirá prevenir los desfalcos, extorsiones, hurtos de cuentas , transferencias ilegales de dinero, etc. para así lograr seguridad en el manejo de las redes informáticas.”, cotejando con la fuente de estadística en base a los sujetos encuestados, sugieren que es imperante la elaboración de un proyecto de ley que incorpore al Fraude Informático como un nuevo delito, pero para que este nuevo delito tenga eficacia y así poder llegar a una condena para los que la cometen, tendrá que estar respaldado por personal idóneo en las investigaciones y peritajes que tengan que realizarse.

Para tener un adecuado debido proceso con pruebas fehacientes en la fase investigativa de la etapa preliminar o preparatoria y tener una investigación exitosa, será necesario tener una capacitación constante y permanente a los investigadores, fiscales, y demás personal perteneciente a la División que se haga cargo de los delitos informáticos y así no tropezar nuevamente en las penumbras habituales de falta de prueba y demostración.

Es por este motivo que surge la necesidad de regular los manejos informáticos que tengan fines específicamente de recolección de datos para extorsionar, desfalcar, hurtar, y realizar transferencias ilegales de dinero, es decir regular la estafa utilizando la manipulación informática y así como vulgarmente se dice “matar dos pájaros de un tiro”.

Por lo tanto, en base a todo lo señalado, el resultado es que la hipótesis queda comprobada debido a que en todas las entrevistas y recolección de teorías de expertos en el tema se llego a la conclusión de que no es lo mismo la manipulación informática que el fraude informático, y que para resolver una denuncia de fraude informático se utilizan dos delitos que son la Estafa y la manipulación Informática por lo tanto se complica la situación para los encargados de impartir justicia tomando en cuenta además que hoy en día varios países vecinos están tipificando en sus códigos este tipo de hechos y nosotros no podemos quedar atrás.

CONCLUSIONES

En base a la hipótesis planteada, se ha realizado la presente investigación si bien con algunos obstáculos, como ser la incipiente bibliografía, pero con la meta de contribuir con la meta de un estudio concreto del fenómeno delictivo que acarrea preocupaciones y dolores de cabeza tanto autoridades del gobierno como a la población en común debido a la comisión del fraude informático, arribando a las siguientes conclusiones:

1. El uso comercial de Internet ha permitido introducir nuevas formas de comunicación como el Facebook, Chat y el correo electronico, donde la mayoria de la poblacion tiene un espacio en la RED.

2. El correo electronico y sobretodo el FACEBOOK, es uno de los medios de comunicación mas utilizados por la red, sin embargo no existe una proteccion efectiva pese a tecnicas como la encriptacion.

3. Considerando el principio de universalidad bajo el cual se rige la Internet y la innegable utilizacion de la red con fines ilicitos es necesaria una regulacion sin dejar de lado el derecho a la privacidad que todo usuario tiene, toda vez que se requiere contar con una seguridad informatica.

4. Los sistemas informaticos constituyen un medio idoneo para la comision de distintas modalidades delictivas sobre todo en lo inherente al Fraude Informatico.

5. La diversidad de criterios en torno al tratamiento y penalizacion de los delitos informaticos, constituye el elemento entorpecedor en el surgimiento de una politica criminal adecuada para los nuevos ilicitos, pese a las recomendaciones emitidas por organismos internacionales de

que los paises cuenten con legislaciones similares, adecuadas a su realidad.

6. Las conductas ilicitas que se cometen en la red se caracterizan por el anonimato, la dificultad de descubrimiento y la obtencion de la prueba, estas conductas deben ser reguladas adecuadamente para aplicar una efectiva sancion, velando siempre el principio de legalidad.

7. La importancia de la implementeacion de politicas, procedimientos y medidas de seguridad, radica en el valor que la informacion representa para las empresas privadas y casi todo el aparato estatal.

8. Las politicas de seguridad deben dirigirse a asegurar la integridad, disponibilidad y confidencialidad de los sistemas informaticos tanto del hardware como del software.

9. El usuario del internet tiene dos cosas de valor cuando navega por la red, su dinero y sus datos.

10. El legislador boliviano debera tener presente las recomendaciones efectuadas por organismos internacionales respecto a la delincuencia informatica y su tratamiento, para enfrentar a este nuevo delito que es el fraude Informatico.

11. Diversos paises han formentado la creacion de organismos policiales especializados en las investigaciones de delitos informaticos dada su naturaleza.

12. La FELCC y Fiscalia paceña no cuenta con una unidad especializada para la investigacion de los delitos informaticos, y solo estan designados a estos casos las divisiones de Propiedades y financieros.

13. El carácter transnacional de los delitos informáticos ponen de manifiesto la necesidad apremiante de una cooperación mundial para modernizar las leyes nacionales, técnicas de investigación, asesoría jurídica y tratados de extradición.

14. Las recomendaciones efectuadas por la ONU y la Comunidad Europea respecto a regular la distribución de la pornografia infantil comercializadas a través de la red, nuestro país esta obligado a la brevedad posible de sancionar este tipo de conductas.

15. No se regula el intrusismo informático como delito autónomo atentatorio contra el derecho a la intimidad.

16. Se regula de manera ambigua el fraude informático en el Art 363 Bis, sin embargo no existe la agravante de que cuando el tipo penal fuera realizado por funcionario público y la inhabilitación correspondiente.

17. Nuestra legislación actualmente no contempla de una manera directa y efectiva las acciones ilícitas que son objeto de estudio, sin embargo las pérdidas económicas pueden ser de gran magnitud, toda vez que más personas se las ingenian para lucrar, hacer daño através del uso de los sistemas informáticos.

18. Por ultimo tenemos que decir que no es lo mismo el fraude Infortmatico que una Estafa o una Manipulacion informatica.

RECOMENDACIONES

Con la esperanza de que la presente investigación se constituya en un aporte investigativo en relación a la delincuencia informática, me permito realizar las siguientes recomendaciones:

1. Desde el punto de vista social es conveniente educar y enseñar a la población sobre el uso correcto de las herramientas informáticas, las conductas prohibidas no solo con el afán de protegerse, sino de no convertirse en un agente de dispersión que pueda contribuir a propagar por ejemplo un virus.

2. Debe evaluarse los riesgos de origen interno o externo y en que medida se desea proteger los bienes para la implementación de una adecuada y eficaz política de seguridad informatica.

3. En el sector empresarial deberán contar con más de un ingeniero en sistemas para las políticas de seguridad con el fin de que si uno falla el otro podrá subsanar el error, asimismo no es prudente que se deposite la confianza en una sola persona sobre la seguridad de la empresa para que no tenga la opción de violar la seguridad del sistema.

4. Si un empleado es retirado de la institucion que fuere ya sea publica o privada se le deberá cancelar el acceso a los recursos disponibles por ejemplo cuentas de usuarios, servicio de acceso remoto, unidades de redes y cambiar las claves de acceso.

5. Adherirnos a los postulados de la ONU en el sentido de unificar la legislación internacional que regule la problemática de la cibernética, por el hecho de que favorece a la multiplicación de autores que utilizan medios informaticos para cometer delitos a sabiendas que no

serán castigadas sus conductas por no estar trpificadas en otro Estado.

6. Promulgación de una Ley que modifique el Codigo Penal vigente e inserte entre los delitos el fraude Informatico en un articulo autonomo para no tropezar con el problema de la subsuncion de dos delitos en un solo hecho como sucede actualmente.

7. Por el carácter especial de los delitos informáticos se constituye en una necesidad la promulgación de una Ley de creación de la Unidad de investigación de la delincuencia en tecnologías de la información como unidad dependiente del Departamento Nacional de Asuntos Criminales. Asimismo la reglamentación correspondiente.

8. Es imprescindible que la Unidad de lnvestigación de la delincuencia en tecnologías de la información este conformada por personal altamente especializado, es decir, Ingenieros en Sistemas, Abogados, Policias, Fiscales con conocimiento de derecho Informatico.

ANTEPROYECTO DE LEY

PROYECTO DE LEY PARA LA INCORPORACION DE LA FIGURA DELICTIVA DEL FRAUDE INFORMATICO EN EL CODIGO PENAL BOLIVIANO

BIBLIOGRAFIA

ANGULO URASTEGUI, J.M.	INTRODUCCIÓN A LA INFORMATICA Edit. Paraninfo. 1987
AGUDELO BETANCUR NODIER	CURSO DE DERECHO PENAL Edic. Nuevo Foro.l998
ALTMARK DANIEL	INFORMATICA Y DERECHO Edit. Depalma. Bs. Aires 1987 Volumen I
AZPILCIJETA HERMILIO TOMAS	DERECHO INFORMATICO Edit. Abeledo p. Bs. Aires 1987
BARBERA MANUEL Y OTROS	INTERNET: TODAS LAS CLAVES PARA NAVEGAR
BUNGE MARIO FILOSOFIA	LA CIENCIA SU METODO Y SU Edit. Siglo veinte, Bs. Aires Argentina 1971
CABANELLAS GUILLERMO	ENCICLOPEDTA JURÍDICA Edit. Heliasta S.R.L. 2001
CAJIAS K., HUA$CAR Y BOLIVIANO, MIGUEL HARB, MIGUEL	APUNTES DE DERECHO PENAL Edit. Juventud, 2da Edic. La Paz Bolivia 1966

CAJIAS K., HUASCAR	CRIMINOLOGIA, Edit. Juventud, quinta edic., La paz Bolivia 1985
CARRAZANA ESTIVARIZ JAIME	COMPUTACION BASICA Edit. Taller Gráfico Hisbol, La Paz Bolivia 1992
CASTILLO M., LUM ALBERTO	ECONOMIA INFORMATICA Instifuto de Investigaciones Económicas U.M.S.A 2001
COMER, MICHAEL J.	EL FRAUDE EN LA EMPRESA Edic. Deusto, Bilbao – España 1987
CORREA CARLOS Y OTROS	DERECHO INFORMATICO Edit. Depalma. Bs. Aires 1987
CRUMLISH CHRISTIAN	DICCIONARIO DE INTERNET Traducción: Jorge Becerra Edit. Mc. Graw Hill. 1996
DRUCKER, PETER E.	LA SOCIEDAD POSTCAPITALISTA Edit. grupo editorial norma en Colombia 1994
ENCICLOPEDIA CETTICO	ENCICLOPEDIA DE INFORMATICA Y COMPUTACION deontología informática Edit. Cultural S.A., España. 1997
ENGELS FEDERICO	EL ORIGEN DE LA FAMILIA LA PROPIEDAD PRIVADA Y EL ESTADO I. Andreev. Edit. Progreso. 1988
FERNANDEZ, DAZA ROBERTO	DERECHO INFORMATICO, Apuntes fotostaticas UMSA 2009

FONTAN B., CARLOS	DERECHO PENAL Parte Especial. XIV Edición. Edit. Abeledo Perrot. Bs. Aires
GARCIA VILLARREAL JUAN Y FERNANDO	AT COMPUTER 286, 386, 486 Edit. Electrónica e informática Srl., Perú 1995
GHERSI CARLOS	DERECHO DE DAÑOS Edit. Abeledo Perrot. Bs. Aires
GUIBOURG RICARDO, JURIDICA ALENDE JORGE Y CAMPANELLA ELENA	MANUAL DE INFORMATICA Edit. Astrea, Bs. Aires Argentina, 1996
HUERTA M. MARCELO Y CLAUDIO LIBANO	DELITOS INFORMATICOS Edit. Jurídica Conosur Ltda.
JIMENEZ ORELLANA, JORGE	MANUAL DE TESIS Taller Gráfico imprenta "Veloz ", Cochabamba – Bolivia 1999.
LLANEZA G., PALOMA	INTERNET Y COMUNICACIONES DIGITALES Barcelona.2000
MAGGIORE GIUSEPPE	DERECHO PENAL Edit. Temis. Vol. II, 1989
MIGUEL H, BENJAMIN	DERECHO PENAL Tomo I PARTE GENERAL Edit. Juventud. 1992
MIGUEL H., BENJAMIN	DERECHO PENAL Tomo II PARTE ESPECIAL Edit. Juventud. 1990
MOLINA FERNANDO HORACIO	DELITOS DE CUELLO BLANCO EN ARGENTINA Edit. Depalma. Bs. Aires 1989

MOSCOSO DELGADO, JAIME	INTRODUCCION AL DERECHO Edit, Universo, La Paz - Bolivia. 1961
OCAMPO DUQUE MARCELA Y OTRO	DERECHO E INFORMATICA Bogotá, D.E. 1987
PFAFFENBERGER, BRYAN	DICCIONARIO PARA USUARIOS DE, COMPUTADORAS E INTERNET, 6ta. Edición, Trad. Oscar A. Palmas V., Prentice-Hall Hispanoamérica, S. A., México, 1996
RAMOS, JUAN M	NUEVO RECURSO CONSTITUCIONAL "HABEAS DATA" EN EL DERECHO INFORMATICO, Edit. Trama Color, 2001
RAMOS, JUAN M.	CONSTITUCIÓN POLÍTICA DEL ESTADO Y DD. HH. Edit. Offset Color S.R.L., 2001
RODRIGUEZ JOSE MANUEL	MANUAL DE PREVENCIÓN DEL FRAUDE Edit. Esoba. España 1991
SOPENA, RAMÓN ILUSTRADO	DICCCIONARIO ENCICLOPEDICO Edit. Ramón Sopena, 3 tomos España. 1950
SPROVIERO H., JUAN	DELITOS DE ESTAFAS Y OTRAS DEFRAUDACIONES Edit. Abaco Tomo I, II
TOFFLER, ALVIN Y TOFFLER, HEIDI	LAS GUERRAS DEL FUTURO Edit Plaza y Janes editores S.A., España 1994
VARGAS FLORES, ARTURO	GUIA TEORICO PRACTICO PARA LA ELABORACIÓN DEL PERFIL DE TESIS,

Facultad de derecho Umsa, 2003

ZORRILLA A., SANTIAGO - TORREZ' MIGUEL — GUIA PARA ELABORAR LA TESIS Edit. McGraw-Hill, México. 1994

LEYES Y CODIGOS

CONSTITUCION POLITICA DEL ESTADO, Edit. UPS, La Paz – Bolivia 2010

CODIGO CIVIL Concordado DL. 12760, Edit. Serrano Ltda. Cochabamba – Bolivia, 2008

CODIGO PENAL BOLIVIANO, Edit. UPS srl, La Paz Bolivia 2010

TESIS CONSULTADAS

CARRION HUGO	PRESUPUESTOS PARA LA INCRIMINACION DEL HACKING (España)
CUSICANQUI SALINAS ANTONIO	LA DELINCUENCIA INFORMATICA U.M.S.A.
OLIVOS L., GRETTEL MARIE	DELIMITACION DEL DELITO INFORMATICO: BIEN JURIDICO PROTEGIDO Y ANÁLISIS DE LA LEGISLACIÓN VIGENTE (Perú - Lima 2001)
TINAJEROS ARCE, ERIKA	BASES JURIDICO PENALES SOBRE SABOTAJE INFORMATICO EMPRESARIAL CONTRA LA INDUSTRIA Y EL COMERCIO U.M.S.A.2001
TOLEDO D. JOSE A.	DELITOS EMERGENTES EN INTERNET Y EL DESAFIO DE CARABINEROS DE CHILE EN LA PREVENCIÓN Y CONTROL EN LA ERA INFORMATICA (Chile)

PERIODICOS CONSULTADOS

EL DIARIO

LA PRENSA

LA RAZÓN

LOS TIEMPOS

PAGINA SIETE

SEMANARIO TECNOLOGÍA.BO

WEBS CONSULTADAS

http ://freenet.sourceforge.net/

http ://www.bufetalmeida.com./textos/hackercrack

http ://www.2.rn.es/merce/ciberamor.html

http ://www.match.com

http ://www. arnal.es/free/noticias

http ://www.delitosinformaticos.com-/articulos/freenet.html

http ://www.elmundo.es/

http;//www.vlex.com

http://bulmalug.net

http ://www.delitosinformaticos.com

http ://publicaciones.derecho.org

http://www.stj-sin.gob.mx/

http : //bufetalmeida.com

http ://control.net/consultoria-inet.html

http ://www.monografias.com

http ://delitosinformaticos.com/trabajos

http ://www.interpol.int

http ://www.htcn.org

http://www.virusprot.com

http ://www.ciberderecho.com

http ://www.Sittel.com

http ://cnnenespañol.com/2011/

http ://www.mir.es/policia

http ://periciascaligraficas.com

http :// Kriptopolis.com…-

http ://www.lawebdelprogramador.com/diccionario

http : //www.angelfire.com

ANEXOS