UNIVERSIDAD AMAZÓNICA DE PANDO

Área de Ciencias Jurídicas Políticas y Sociales

Carrera de Derecho

TESIS DE GRADO

"EL DELITO CIBERNÉTICO DE SUPLANTACIÓN DE IDENTIDAD EN LA LEGISLACIÓN NACIONAL"

TESIS PRESENTADA PARA OPTAR EL TÍTULO ACADÉMICO DE LICENCIATURA EN DERECHO

POSTULANTE: Roberto Genaro Huanca Choquetarqui

TUTOR: Dr. Oscar Melgar Saucedo

COBIJA – PANDO- BOLIVIA
2013

DEDICATORIA

El presente trabajo la dedico a nuestro Creador, por ser quien guía mi vivir y forma parte de mis triunfos y derrotas

A mi compañera y Amiga Yilda Paruma y a mis dos hijos Brandon Henrry y Montserrat Cameron Huanca Paruma, quienes son la motivación para una constante superación, gracias a ellos por descuidarlos, pues el logro de objetivos implica sacrificios… gracias por su comprensión

AGRADECIMIENTO

A la Universidad Amazónica de Pando, porque en sus aulas adquirí los conocimientos que plasmaré en mi vida profesional.

Al Comando Departamental de Policía de Pando, por abrirme las puertas para una vida profesional y haberme permitido profesionalizarme en derecho.

Al. Lic. Abog. Oscar Melgar Saucedo y al Lic. Franz Ricardo Tambo, por sus aportes valiosos y su constante comprensión cuyos aportes oportunos permitieron culminar el presente trabajo de investigación.

A todos los docentes que en mi inculcaron los conocimiento jurídicos necesario A mis camaradas del Verde Olivo por su cooperación en forma directa e indirecta.

ÍNDICE GENERAL

1. INTRODUCCIÓN

El desarrollo de la humanidad está acompañado a la transmisión de la información de forma continua. Realizando una retrospectiva aun viene a la memoria las señales de humo o los destellos con espejos, y más recientemente los mensajes transmitidos a través de cables utilizando el Código Morse, o la propia voz por medio del teléfono. La humanidad no ha cesado en la creación de métodos para procesar información. Con ése fin nace la informática, como ciencia encargada del estudio y desarrollo de estas máquinas y métodos, y además con la idea de ayudar al hombre en aquellos trabajos rutinarios y repetitivos, generalmente de cálculo o de gestión.

A la par del desarrollo de la Informática se observa un avance en cuanto al manejo del Internet como una Tecnología que pondría la cultura, la ciencia y la información al alcance de millones de personas de todo el mundo, lo que conlleva a la aparición de delincuentes que encontraron el modo de contaminarla y lo que es peor impunemente. Al mismo tiempo que la Internet supuso un increíble avance en el complejo universo de las nuevas tecnologías, (NTIC´s), también se configuró como un nuevo instrumento y un medio para la comisión de delitos, estafas y fraudes. Igualmente trajo consigo la vulneración de los sistemas de seguridad y la invasión en la intimidad de las personas (acceso a bases de datos, intromisiones ilegítimas en las cuentas de correo electrónico, etc.). Este desarrollo de las tecnologías informáticas ofrece un aspecto negativo: Ha abierto la puerta a conductas antisociales y delictivas.

Por todo ello la presente investigación pretende priorizar la no regulación de los delitos informáticos cometidos en Bolivia, debido al creciente y significativo avance que ha generado el desarrollo, difusión y uso generalizado de la informática y el internet y su reciente impacto en la sociedad boliviana, provoca 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. Por ello **"El delito cibernético de suplantación de identidad en la legislación nacional"** llenará un vacío jurídico traducido en acciones u omisiones típicas, antijurídicas

y culpables realizadas por medios informáticos, es decir los actos como la **suplantación de identidad,** estafas financieras a personas o empresas, insultos y amenazas, hasta delitos de pornografía infantil y pedofilia. Tendrían una mayor penalidad y no como ocurre actualmente solo son considerados como delitos comunes, establecidos en el Código Penal y la ley de telecomunicaciones pero carecen de una ley específica.

La Investigación está dividida en Seis Capítulos. El Capítulo I Marco Metodológico enmarca la delimitación, objetivos, planteamiento del problema y el tipo de investigación aplicada. El Capítulo II describe el Marco Teórico y Doctrinario en el que se sustenta la misma. El Capítulo III. Realiza una descripción pormenorizada de los diferentes organismos Internacionales inmersos en la problemática, el análisis pormenorizado de Marco Jurídico Nacional, concluyendo con la legislación comparada de países en los que existe un avance y desarrollo sobre la temática. El Capítulo IV. Marco Práctico, en la que se realiza el Trabajo de Campo su análisis interpretación y descripción gráfica. El Capítulo V desarrolla Propuesta en que se presenta la ampliación de los delitos de suplantación electrónica, que debería ser implementada para subsanar este vació Jurídico, y finalmente, El Capítulo VI. Se arriba a la Conclusiones y Recomendaciones a las que se llega.

Las actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes, son insuficientes pues, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras y crecimiento constante del número de delitos informáticos, ha creado la necesidad de una regulación penal acorde a los cambios y avances tecnológicos.

CAPITULO I
MARCO METODOLÓGICO

1.1 ANTECEDENTES

Actualmente, tanto en la organización y administración de empresas privadas o públicas, como en la investigación científica, en la producción industrial, en el comercio. La contabilidad, los procesos bancarios, el estudio, el ocio, etc., la informática es una herramienta esencial. Sin embargo, junto a las innegables ventajas que presenta, comienzan a aparecer algunos aspectos negativos producto de la "criminalidad informática". La manipulación fraudulenta de computadoras con fines de lucro, la destrucción de programas o datos y el acceso o la utilización indebida de la información, que puede afectar la privacidad son algunos de los métodos relacionados con el procesamiento electrónico de datos, mediante los cuales es posible obtener grandes beneficios económicos o causar importantes daños morales y/o materiales.

En este sentido, el área temática de la presente investigación está constituido por el Derecho Penal, siendo el objeto de estudio de la misma los delitos cibernéticos que consisten en acciones u omisiones típicas, antijurídicas y culpables realizadas por medios informáticos, es decir los actos como la suplantación de identidad, estafas financieras a personas o empresas, insultos y amenazas, hasta delitos de pornografía infantil y pedofilia. De forma más específica, dentro de ese ámbito de los delitos informáticos, la presente investigación se enfoco en el estudio del delito de "SUPLANTACIÓN DE IDENTIDAD" que aun constituye un vacío jurídico en la legislación nacional ya que en Bolivia los delitos informáticos son tratados como delitos comunes, están incluidos en el Código Penal y la ley de telecomunicaciones pero carecen de una ley específica.

En el marco de lo expuesto y los desafíos del entorno, el presente trabajo de investigación surge de la necesidad de nuevas iniciativas de carácter jurídico para combatir la delincuencia a través de la modernización de la normativa vigente.

La investigación se desarrolló de acuerdo a los lineamientos de la metodología de la investigación, la estructura y formato exigidos por la Universidad Amazónica de Pando.

1.2. PLANTEAMIENTO DEL PROBLEMA.

¿Qué instrumento legal o normativo será necesario desarrollar e implementar para regular el vacío jurídico en torno a la transgresión de suplantación de identidad en el ámbito de los delitos informáticos?

1.3. OBJETIVO DE LA INVESTIGACIÓN.

1.3.1. Objetivo General

Formular un anteproyecto de ley para tipificar e incorporar al Código Penal el delito de suplantación de identidad electrónica en el ámbito de los delitos informáticos.

1.3.2. Objetivos Específicos

- Establecer el Marco Conceptual y Doctrinario sobre la problemática de la suplantación de identidad como delito informático.
- Analizar las convenciones internacionales, la normativa legal comparada y nacional existente sobre los delitos informáticos y de forma especial sobre el delito de suplantación de identidad.
- Efectuar el trabajo de campo para identificar la opinión respecto a la solución del vacío legal en cuanto se refiere al delito de suplantación de identidad electrónica.
- Formular las bases de la propuesta de la Ley para tipificar e incorporar la suplantación de identidad como delito informático en el actual Código Penal.

1.4. JUSTIFICACIÓN:

Las Empresas, personas particulares e incluso el Estado, se ven afectadas por la comisión de actos Ilícitos a través de la apropiación de su identidad digital, no solo con grandes pérdidas económicas, sino también con atentados a su privacidad y honor, entre

otros. Como se puede observar las categorías que definen este delito informático son complejas y pueden incluir delitos tradicionales como el fraude, el robo, chantaje, falsificación y la malversación de caudales públicos en los cuales ordenadores y redes han sido utilizados. La desprotección de la sociedad en un momento de avance tecnológico acelerado debe subsanarse a través de la modernización de la normativa acorde al tiempo y las necesidades de la sociedad en que vivimos.

Por otro lado la apropiación de la identidad digital ya ha generado grandes pérdidas económicas en nuestro medio, tanto para particulares como para instituciones públicas, a través del fraude, el robo, chantaje, falsificación y la malversación de caudales privados y públicos. Por lo tanto es necesario proteger a la sociedad y al Estado de la comisión de este tipo de delitos.

Desde una perspectiva estrictamente jurídica, los delitos informáticos están incluidos en el Código Penal "CAPITULO ONCE, ARTÍCULOS 363 bis. Y 363 ter.", pero de forma incompleta y carente de reglamentación. Por lo tanto existe un vacío jurídico que limita al Órgano Judicial para poder sancionar por la comisión de este tipo de Actos Ilícitos, relacionados con las nuevas tecnologías en nuestro país lo que está acorde al principio Jurídico: *"nullapena sine previalege"*.

1.5. DISEÑO METODOLÓGICO:

Como métodos generales se empleará el método analítico deductivo y el analítico inductivo que se aplico a la observación documental y a la investigación empírica.

1.5.1. Tipo de investigación

El nivel de la presente investigación corresponde al de los estudios exploratorios descriptivos, es decir la caracterización de un fenómeno o situación concreta para identificar sus rasgos inherentes más diferenciadores.

1.5.2. Métodos y técnicas de investigación:

Se utilizó el método de observación documental y de investigación empírica (encuestas) producido los datos de hechos y registrados, descritos e interpretados. Las técnicas a empleados en la recolección de datos que fueron las encuestas estructuradas. Para la interpretación de los mismos, se analizo el contenido de las encuestas, para objetivizar los planteamientos y las necesidades del ámbito de estudio. Los instrumentos constaron de encuestas estructuradas (cuestionarios cerrados) sobre los ámbitos de interés, recolectado la opinión especializada de los señores Fiscales del Ministerio Público, investigadores de la FELCC. Y docentes de derecho penal, de la ciudad de Cobija. Los instrumentos para el procesamiento de los datos constaron de cuaderno de notas para anotaciones y registro de las observaciones y cuadro de observaciones de todas las encuestas realizadas. Finalmente, la información fue trasladada para su graficación. El análisis e Interpretación de los datos consistió en medir el porcentaje de las respuestas para formar un cuadro comparativo de la opinión y realizar la inducción correspondiente.

1.5.3. Método Teórico:

Se utilizará el método de observación documental y de investigación empírica para producir los datos de hechos y registrarlos, describirlos e interpretarlos.

1.5.4. Técnicas:

Las técnicas a emplear para la recolección de datos será la de encuestas estructuradas, para la interpretación de los mismos será el análisis de contenido de las encuestas, permitiéndonos objetivizar los planteamientos y las necesidades del ámbito de estudio.

1.6. DELIMITACIÓN DE LA INVESTIGACIÓN:

1.6.1. Delimitación Temporal.

La investigación corresponde al periodo de la gestión de 2012.

1.6.2. Delimitación geográfica o especial:

Toda la jurisdicción del Estado Plurinacional de Bolivia, sin embargo el trabajo de investigación se realizo en la ciudad de Cobija.

1.6.3. Delimitación Temática:

En la presente investigación se utilizaron doctrinas y técnicas de la Ciencia del derecho en el estudio de los delitos de suplantación de identidad en el ámbito de los delitos electrónicos.

CAPÍTULO II
MARCO TEÓRICO

2.1. MARCO CONCEPTUAL

2.1.1. Derecho Informático

Las sociedades humanas se caracterizan por el constante cambio, el que cada día sorprende más por su rapidez y profunda incidencia en el desarrollo de patrones de conducta social, creando entre las personas nuevos modos de interacción. Sin embargo, no se está únicamente en presencia del progreso científico o tecnológico, sino que el cambio involucra las creencias, las actitudes psicológicas, el ámbito económico y político; en suma, la forma de convivir en el mundo. Es decir, se está viviendo un verdadero cambio social que modifica irreversiblemente los modos de conducta en sociedad.

Sin lugar a dudas, estos cambios sociales profundos se tienen que reflejar a través de modificaciones serias en el ordenamiento jurídico, como sucede por ejemplo, con el surgimiento de la legislación medioambiental o las normas que rigen a las tecnologías de la información. Ante ello, la rama del Derecho no puede negarse a la capacidad de interpretar mejor las necesidades humanas y de adaptarse en forma más perfecta a lo que de él se requiere para el bien común, la paz, la justicia y el progreso.([1])

La revolución tecnológica ha redimensionado las relaciones entre los hombres. Se está ante una sociedad donde las tecnologías de la información han llegado a ser la figura representativa de la cultura, hasta el punto de que para designar el marco de la convivencia se alude reiteradamente a la expresión *Sociedad de la Información.*([2])

[1] NUÑEZ PONCE Julio, *Derecho informático.* Editores Marsol. El Derecho Informático: concepto y diferencias con la informática jurídica. Autonomía y metodología del Derecho Informático. 2007: 20–26.
[2] SONI Mariano, *Compilación de Tratados en Materia de Propiedad Intelectual y Poderes Aplicables en los Países del Continente Americano.* Edición de la Asociación Interamericana de Propiedad Industrial ASIPI. 1995.

2.1.2. Antecedentes del Derecho Informático

Detrás de todo este desarrollo Tecnológico, descansa la Información como objeto de dicha revolución. La información ya era valiosa en el pasado, significaba encontrarse en una situación ventajosa respecto a quienes no la tenían. Pero en el presente su valor se acrecienta, ya que antes no existía la posibilidad de convertir informaciones parciales y dispersas en informaciones en masa y organizadas; de interrelacionar esa información y de procesarla con rapidez, como ocurre hoy, en la sociedad de la Información.

En definitiva, lo que ocurre es que esa información cada vez aporta más conocimiento, que es lo verdaderamente importante y que quien dispone de conocimiento tiene poder.

Frente, a las cada vez mayores repercusiones de la Informática en el Derecho muchos de los problemas que se suscitan no se satisfacen con las soluciones jurídicas tradicionales, muchas de ellas insuficientes y obsoletas hoy en día, debido a que los conceptos y categorías básicas de la ciencia jurídica, que surgieron en la edad moderna y en la codificación actual, han variado.

Tanto el Derecho, como la Informática, puede ser objeto formal y objeto material uno de otro. Cuando el *Derecho* es la materia estudiada por la *informática*, entonces se tiene la *Informática Jurídica*, ciencia que está permitiendo un vasto desarrollo de la eficiencia estatal, agilizando, optimizando y simplificando las labores judiciales, legislativas y ejecutivas.([3])

El futuro de la Informática Jurídica es muy prometedor. A manera de ejemplo se citará a los hoy ya comunes software legales, útiles para localizar normas, jurisprudencia y doctrina; existen técnicos que trabajan para que en el futuro estos programas sean capaces de ubicar automáticamente cualquier incongruencia constitucional o legal, por ejemplo, un proyecto de reglamento.

[3] In bis idem.

Las ventajas de inmediación y comunicación que facilita la Informática han sido ampliamente aprovechadas en los países del primer mundo, quienes aspiran permitir, en un plazo no muy lejano, que sus ciudadanos realicen cualquier trámite legal, como gestionar permisos, presentar pruebas, balances, declaraciones de impuestos, obtener certificados de propiedad, mercantiles, sanitarios; todo desde un cómodo asiento de su casa o, si se prefiere, desde la cálida arena de la playa, mientras se asolean, a través de su portátil conectada a la red sin cable alguno.

Ya hoy se ve en Internet desordenadas las antiguas estructuras judiciales, donde van ganando terreno, con una agresividad que espanta, medios alternativos de justicia como el arbitraje on-line.[4]

Se decía que tanto el Derecho, como la Informática, pueden ser objeto formal y objeto material, uno de otro. Cuando el *Derecho* no es la materia estudiada, sino el punto de vista desde el cual se estudia la *Informática,* entonces tenemos el *Derecho Informático.* Aquí la *Informática* ha perdido su calidad de ciencia y pasa a ser la cosa estudiada.

2.1.3. Definición de Derecho Informático

La palabra *Informática* tiene un significado cada vez más tangible, más cercano para el hombre contemporáneo, lo que no significa que sea más preciso. Evoca en la memoria múltiples imágenes de computadoras, redes, antenas, correos electrónicos, programas de software, algunos sitios. Por otro lado, no aparecen ciertos medios de comunicación como lo son un televisor, una radio, la prensa escrita.

Quizá se comience a interrogarse, si los impuestos forman parte del Derecho Informático; así como si las normas de la publicidad, también son Derecho Informático y el Derecho a la Intimidad.

---

[4] Edgar, Salazar, *Cibernética y Derecho Procesal Civil,* Ediciones Técnico- Jurídicas. Caracas. 1979. p. 264.

Es aquí donde la filología lanza una primera interrogante que permite mantenerse a flote. La palabra española *Informática* deriva del vocablo francés *informatique*, que a su vez es un compuesto contracto de *información y automatique*.

La Informática alude directamente al tratamiento automático de la Información. En este orden de ideas el diccionario de la Real Academia de la Lengua Española de 1984 definía la voz *Informática* como el "conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la Información por medio de calculadoras electrónicas."[5]

Actualmente, con el avance de la técnica, fue preciso cambiar las palabras *calculadoras electrónicas* por *ordenadores*, pero el resto la definición se mantuvo intacta.

Informática es la ciencia del tratamiento sistemático y eficaz, realzado especialmente con máquinas automatizadas, de la Información, contemplada como vehículo del saber humano y de la comunicación de los ámbitos técnico, económico y social. (Documento IBI).

Se define también como "La disciplina que estudia el fenómeno de la Información, la elaboración, trasmisión y utilización de la Información principalmente, aunque no necesariamente, con la ayuda de ordenadores y sistemas de telecomunicación como instrumentos".([6])

"Informática es la aplicación racional y sistemática de la información para el desarrollo económico, social y político" (Altmark).

Una segunda definición se la obtiene combinando el objeto material de la ciencia, con el formal, resulta que el Derecho Informático es aquel conjunto de normas, principios e instituciones que regulan el tratamiento automatizado de la información.([7])

---

[5] Ver: Diccionario de la Lengua Española. Real Academia Española. Madrid - España: Ed. Espasa Calpe. 1992.
[6] GARCÍA PÉREZ, Inmaculada, , Especialista en: *Derecho Nuevas Tecnologías.* 14 de Febrero de 2002.
[7] GARCÍA PÉREZ Inmaculada, , Especialista en: *Derecho Nuevas Tecnologías.* 14 de Febrero de 2002.

Ambas definiciones concuerdan plenamente con otras como la de Altmark, quien estima que el *Derecho Informático es el conjunto de normas, principios e instituciones que regulan las relaciones jurídicas emergentes de la actividad Informática.*

2.1.4. Naturaleza Jurídica del Derecho Informático

Al respecto, según encuentros sobre Informática realizados en Facultades de Derecho en España a partir de 1.987, organizados por ICADE, siempre surgían problemas a la hora de catalogar al Derecho Informático como rama jurídica autónoma del Derecho o simplemente si el Derecho Informático debe diluirse entre las distintas ramas del Derecho, asumiendo cada una de estas la parte que le correspondiese.

En el VI Congreso Iberoamericano de Derecho e Informática celebrado en Montevideo - Uruguay, en 1998, se expusieron las razones por las cuales el Derecho Informático es una rama autónoma del Derecho.

Desde aquel momento surgieron diferentes criterios, algunos afirmaban que el Derecho Informático nunca comprendería una rama autónoma del Derecho, por cuanto dependía en su esencia de otras ramas del Derecho, otros comentaban acerca del Derecho Informático como una rama potencial del Derecho, debido a su insuficiente contenido y desarrollo.

Para hablar propiamente de la autonomía de una rama del derecho se necesitan ciertas características: la existencia de campo normativo, docente, institucional y científico, con la finalidad de que se dé un tratamiento específico de estos conocimientos determinados y, desde ese primer momento en que exhibí las razones de la autonomía del Derecho Informático.

Por exigencias científicas, por cuanto un conjunto de conocimientos específicos conllevan a su organización u ordenación, o por razones prácticas que llevan a la

separación del trabajo en vías de su organización, se encuentra una serie de material de normas legales, doctrina, jurisprudencia, que fueron catalogadas y ubicadas en diversos sectores o ramas.

Dicha ordenación u organización del Derecho en diversas ramas, tiene en su formación la influencia del carácter de las relaciones sociales o del contenido de las normas, entonces se van formando y delimitando en sectores o ramas, como la del Derecho Civil, Penal, Constitucional, Contencioso Administrativo, sin poderse establecer límites entre una rama jurídica y otra, por cuanto, existe una zona común a todas ellas, que integran a esos campos limítrofes. De manera que, esta agrupación u ordenación en sectores o ramas da origen a determinadas Ciencias Jurídicas, que se encargan de estudiar a ese particular sector que les compete.([8])

Generalmente, el nacimiento de una rama jurídica surge a consecuencia de cambios sociales reflejados en las soluciones normativas al transcurso de los años. Pero resulta que, en el caso del Derecho Informático no hubo ese transcurrir del tiempo en los cambios sociales, sino que el cambio fue brusco y en poco tiempo, como consecuencia del impacto de la Informática en la sociedad, lográndose sociedades altamente informatizadas, que sin la ayuda actual de la Informática colapsarían.

En este orden de ideas, es menester entonces concluir que en el Derecho Informático sí existe legislación específica, que protege al campo informático. Tal vez no con tanta trayectoria y evolución como la legislación que comprenden otras ramas del Derecho, pero si existe en el Derecho Informático legislación basada en leyes, tratados y convenios internacionales, además de los distintos proyectos que se llevan a cabo en los entes legislativos de nuestras naciones, con la finalidad del control y aplicación lícita de los instrumentos informáticos.

[8] PEÑARANDA QUINTERO Héctor Ramón, **,** (Abogado – Magíster en Gerencia Tributaria – Doctor en Derecho – Presidente de la Organización Mundial de Derecho e Informática – Autor del Libro IUSCIBERNÉTICA: Interrelación entre el Derecho y la Informática, Juez del Tribunal de Protección del Niño y del Adolescente de la Circunscripción Judicial del Estado Zulia) - Maracaibo – Venezuela. 2007: 23

Con respecto a las instituciones propias que no se encuentren en otras áreas del Derecho (campo institucional), se encuentra el contrato informático, el documento electrónico, el comercio electrónico, delitos informáticos, firmas digitales, habeas data, libertad informática, entre otras, que llevan a la necesidad de un estudio particularizado de la materia (campo docente), dando como resultado las investigaciones, doctrinas que traten la materia (campo científico). En efecto, se pueden conseguir actualmente grandes cantidades de investigaciones, artículos, libros, e inclusive jurisprudencia que esté enmarcada en la interrelación entre el Derecho y la Informática, creándose sus propios principios e instituciones, como se ha constatado en los Congresos Iberoamericanos de Derecho e Informática.

Por lo tanto, no hay excusa, ni siquiera en un país donde el grado de informatización sea bajo para que se obvie la posibilidad de hablar del Derecho Informático como rama jurídica autónoma del Derecho, si bien se puede llegar a ella, no sólo por la integración de las normas jurídicas, sino también para su aplicación diversa, cuando en un sistema jurídico existan vacíos legales al respecto, se toma cuenta ante el aumento de las ciencias dogmática-jurídicas, el Derecho es un todo unitario, puesto que las normas jurídicas están estrechamente vinculadas entre sí ya sea por relaciones de coordinación o de subordinación, con lo que se concluye que para la solución de una controversia con relevancia jurídica, se puede a través de la experiencia jurídica buscar su solución en la integración de normas constitucionales, administrativas, financieras, entre otros o llegar a la normativa impuesta por convenios o tratados internacionales que subordinan a la presión supranacional.

2.1.5. Fuentes del Derecho Informático

Entre las fuentes del Derecho Informático se tienen las siguientes:

Fuentes interdisciplinarias:

Son aquellas fuentes dentro de la disciplina jurídica, son fuentes propias entre las que se tienen ([9]):

- Legislación Informática, son un conjunto de disposiciones, de regulaciones de normas obligatorias que regulan el mundo y las relaciones de la Informática.

- Doctrina Informática, es un conjunto de ideas, opiniones sobre el derecho, teorías que se elaboran sobre el tratamiento de la Informática que este conjunto de opiniones puede ser teatro, libros, artículos, estudios, etc. y de estos se obtiene leyes.

- Jurisdicción Informática, son los fallos, sentencias, resoluciones que tienen contenidos informático, en síntesis son fallos con relación a temas Informáticos.

    - Antes la principal fuente fue la Costumbre.
    - Hoy en día la principal fuente es la Legislación.
    - La principal fuente del derecho Informático es la Jurisprudencia.

Fuentes Transdisciplinarias

Entre las que se puede mencionar[10]:

- **Sociología,** encargada de estudiar los fenómenos que se dan en la sociedad, dando pautas de que dirección se deben tomar los legisladores en las leyes referidas a la informática y su gran crecimiento.

- **Economía,** estudia los fenómenos económicos, y las relaciones de producción.

[9] UNED. Revista, Iberoamericana de Derecho Informático. XIV Tomos. España. 1.996.
[10] GIRALDO Jaime, *Informática Jurídica Documental*. Temis. Colombia. 1990. p. 192.

- **Filosofía,** indica cómo serán las relaciones con las normas jurídicas, da la señal de la ley perfecta, un prototipo de ley optimizadora para el razonamiento, la base de la informática es la lógica formal.

- **Estadística,** maneja datos, información, la ordena, clasifica, sistematiza, procesa, analiza, etc.

- **Política Económica,** si se habla de economía política se habla de una estrategia, de una planificación para llegar a un objetivo.

2.2. LA INFORMÁTICA JURÍDICA

La Informática constituye un fenómeno-ciencia, que ha logrado penetrar en todos los ámbitos o áreas del conocimiento humano, y siendo el Derecho una ciencia, por cuanto constituye un área del saber humano, reflejándose en un conjunto de conocimientos, pues, no cae en la excepción de ser tratada por la Informática, dando lugar en términos instrumentales a la Informática jurídica, que consiste en una ciencia que forma parte de la Informática, que al ser aplicada sobre el Derecho busca el tratamiento lógico y automático de la información legal.

La Informática Jurídica ha sufrido una serie de variaciones a lo largo de la evolución de la propia Informática, pero su nacimiento es demarcado en el año 1959 en los Estados Unidos.([11])

Tuvo su comienzo cuando en los años cincuenta se desarrolla las primeras investigaciones para buscar la recuperación de documentos jurídicos en forma automatizada. De esta manera, se comienzan a utilizar las computadoras u ordenadores ya no para trabajos matemáticos, sino también para los lingüísticos.

[11] GUIBOURG, Ricardo A., *Manual de informática jurídica,* Astrea, Capítulo IV – Informática Jurídica de gestión. 1996. p. 99.

Fue en la Universidad de Pittsburg, Pennsylvania, a través del Health Law Center, donde el Director llamado John Horty concibió la idea de crear un mecanismo a través del cual se pudiera tener acceso a la información legal de manera automatizada.

La informática es el conjunto de conocimientos científicos y técnicos que se ocupan del tratamiento de la información por medio de ordenadores electrónicos.([12])

También se puede decir que es un conjunto de conocimientos científicos y de técnicas, que hacen posible el tratamiento automático de la información por medio de computadoras. La informática combina los aspectos teóricos y prácticos de la ingeniería, electrónica, teoría de la información, matemáticas, lógica y comportamiento humano. Los aspectos de la informática cubren desde la programación y la arquitectura informática hasta la inteligencia artificial y la robótica.([13])

2.2.1. Definición de Informática Jurídica

La Informática jurídica consiste en una ciencia que forma parte de la Informática, determinado como la especie en el género, y se aplica sobre el Derecho; de manera que, se dé el tratamiento lógico y automático de la información legal.

Es una ciencia que estudia la utilización de aparatos o elementos físicos electrónicos, como la computadora, en el Derecho; es decir, la ayuda que este uso presta al desarrollo y aplicación del Derecho.

En otras palabras, es ver el aspecto instrumental dado a raíz de la Informática en el Derecho. Descubriendo así las técnicas y conocimientos para la investigación y desarrollo de los conocimientos de la Informática para la expansión del Derecho, a través de la

[12] NUÑEZ PONCE, Julio; *Derecho informático*, Editores Marsol, Derecho Informático: concepto y diferencias con la informática jurídica. Autonomía y metodología del Derecho Informático. 2001. p. 20–26.
[13] GUIBOURG, Ricardo A., *Manual de informática jurídica*, Astrea, Capítulo IV – Informática Jurídica de gestión. 1996. p. 99.

recuperación jurídica, como también la elaboración de material lingüístico legal, instrumentos de análisis, y en general el tratamiento de la información jurídica.([14])

Es importante recordar, que la Informática jurídica como disciplina dentro de la Iuscibernética –que constituye el marco mediato entre la relación Derecho e Informática, y que la misma forma parte de la cibernética como ciencia general- han hecho posible el desarrollo de ciencias que al mezclarse posibilitan un mejor desarrollo y tratamiento de la comunicación de las mismas, como se refleja en esta relación entre el Derecho e Informática de las cuales se desprenden ciertas disciplinas como lo son la Informática Jurídica, el Derecho Informático, la Jurimetría, Modelística Jurídica, entre otras.

2.2.2. El Ciberespacio

El ciberespacio, es un mundo virtual en el que los defectos y malos hábitos del ser humano se reproducen rápidamente, a la misma velocidad que permite las computadoras así como en todo el planeta ampara la rápida transmisión de mensajes y permite el acceso a toda la información introducida en Internet.[15]

Al igual que las ventajas que acarrea esto, se asocian las deformaciones y el mal trato que se le da a esta herramienta en cualquier sistema, que ratifica nuevamente que el mal no está en los medios sino en las personas que lo utilizan. La necesidad de prevenir y sancionar estos malos usos en Internet, que es la cuna de la delincuencia por lo que se hace necesario determinar las alteraciones más frecuentes que se producen para cortar de raíz esta modalidad delictiva.

2.2.3. Definición de Delitos Informáticos

Dar un concepto sobre delitos informáticos no es una labor fácil y esto en razón de que su misma denominación alude a una situación muy especial, ya que para hablar de *delitos* en el sentido de acciones tipificadas o contempladas en textos jurídico-penales, se

[14] MÁRQUEZ; José Antonio, *La contratación electrónica en los códigos civiles*, Cátedra de Informática Jurídica TEC de Monterrey, México. Disponible en: http://www.mty.itesm.mx Junio del 2003. Recuperado el: 15-09-09.
[15] GUIBOURG; Ricardo A., *Manual de informática jurídica*, Astrea, La historia: aceleración y resistencias (pág. 1); Derecho. Cibernética. Informática. 1996. p. 9 – 12.

requiere que la expresión delitos informáticos, este consignada en los códigos penales, lo cual en Bolivia al igual que en muchos otros, no ha sido objeto de tipificación aún; solo con excepción del estado de Sinaloa que ya incluyó esta modalidad.

Actualmente, se está produciendo un intenso debate respecto a la necesidad de prevenir y sancionar estos malos usos en el Internet, y el objetivo de este trabajo de investigación es sugerir la inclusión dentro del Código Penal Boliviano, un proyecto de ley que tipifique y penalicé el mal uso de la red, porque cada día aparecen nuevos métodos de vulneración de los sistemas, aparte de los fraudes y todo el mal uso que se está dando al Internet por lo tanto se hace necesario que también la leyes se deben mover con la tecnología, para mantener una actualización porque tanto, en el campo de la informática así como el derecho todo cambia continuamente.

En definitiva, con la ayuda de las nuevas tecnologías, aparecen nuevos delitos y nuevas formas de comisión de delitos. Ante esto el legislador no se puede quedar de brazos cruzados y no regular este aspecto de la informática.

2.2.4. Evolución de los delitos informáticos

El Internet ha creado nuevas posibilidades delictivas lo que ha propiciado a su vez la necesidad de regulación por parte del derecho, ya que la tecnología informática en la actualidad abarca a todos los aspectos de la vida cotidiana; (en la industria, el comercio, la administración pública, etc. En este sentido, la manipulación fraudulenta de computadoras, con ánimo de lucro, la destrucción de programas y datos así como el acceso y utilización indebida de la información como la suplantación de identidad con fines ilícitos, son algunos de los principales retos para la pertinente regulación jurídica. Respecto a la regulación de estos delitos, en un primer momento las figuras delictivas tradicionales fueron utilizadas, adaptándolas al nuevo objeto de regulación, en particular, los delitos patrimoniales, pero, como veremos más adelante, éstas figuras delictivas tradicionales no ofrecen una delimitación típica completa frente a las nuevas conductas

delictivas, razón por la cual en muchas legislaciones se tiende a crear tipos penales especiales referidos al delito informático; siguiendo esta misma línea se encuentra nuestro Código Penal, donde, no obstante, aún resulta difícil precisar jurídicamente tales conductas dado el carácter excesivamente genérico de las nuevas normas incorporadas.

La importancia de las conductas delictivas a nivel internacional puede observarse con claridad en la siguiente cita:

A nivel mundial los delitos informáticos cuestan alrededor de 114.000 millones de dólares al año, y en 2010 afectaron a 431 millones de personas, Según el Informe sobre Delito Cibernético de Symantec.74 millones de personas en Estados Unidos fueron víctimas de delitos informáticos en 2011, lo que supuso 32.000 millones de dólares en pérdidas financieras directas. En China, el costo del delito cibernético llego a los 25.000 millones de dólares. En Brasil llegó a los 15.000 millones y en India a los 4.000 millones. Según Symantec, más de dos terceras partes de los usuarios de Internet fueron víctimas de la delincuencia cibernética en algún momento de sus vidas, lo que resulta en más de un millón de víctimas del cibercrimen al día. La tasa de delitos informáticos en 2011 trepó incluso en China al 85% y en Sudáfrica al 84%. El cibercrimen ha supuesto, un costo mayor que el del narcotráfico (288 mil millones de dólares)". (Gelhard:2011:101-105)

Los expertos en seguridad informática indican que en la actualidad es más factible ser víctima de un delito cibernético que de uno físico, y que una de las razones por las que somos más vulnerables a este tipo de delitos es la falta de conciencia del riesgo que corremos cada día, así como el retraso de la adecuación normativa al avance tecnológico. (Gelhard: 2011: 111). Es importante resaltar que en lo anotado solo se establece la estadística del daño económico y no así de otros bienes jurídicos no protegidos.

2.2.5. Definición de Internet

Los autores consultados, señalan que el Protocolo de Internet (IP) y el Protocolo de Control de Transmisión (TCP) fueron desarrollados inicialmente como una idea en 1969, posteriormente en 1973 por el informático estadounidense Vinton Cerf como parte de un proyecto dirigido por el ingeniero estadounidense Robert Kahn y patrocinado por la Agencia de Programas Avanzados de Investigación (ARPA, siglas en inglés) del Departamento Estadounidense de Defensa. Internet comenzó siendo una red informática de ARPA (llamada ARPANET) que conectaba redes de ordenadores de varias universidades y laboratorios de investigación en Estados Unidos. La World Wide Web fue desarrollada en 1989 por el informático británico Timothy Berners-Lee para Organización Europea para la Investigación Nuclear, más conocida como CERN.([16])

A principios de 1980, las redes más coordinadas, como CSNET (red de ciencias de cómputo), y BITNET, empezaron a proveer redes de alcance nacional, a las entidades académicas y de investigación, las cuales hicieron conexiones especiales que permitieron intercambiar información entre las diferentes comunidades. En 1986, se creó la NSFNET (Red de la Fundación Nacional de Ciencias), la cual unió en cinco macro centros de cómputo a investigadores de diferentes Estados de Norte América, de este modo, esta red se expandió con gran rapidez, conectando redes académicas a más centro de investigación, remplazando así a ARPANET en el trabajo de redes de investigación. ARPANET se da de baja en marzo de 1990 y CSNET deja de existir en 1991, cediendo su lugar a INTERNET.([17])

2.2.6. Los Documentos Informáticos

La voz Documento, deriva de la palabra *Dekos*, empleada por lo general en las esferas religiosas. Denotaba el gesto de las manos extendidas, tanto para ofrecer como

[16] ATHENIENSE, Alexandre, *Auto-Aplicaçao do Código do Consumidor Brasileiro nas Transaçoes de Bens Corpóreos pelo Comércio Electrònico na Internet*, III Congreso de Derecho Informático. Disponible em: http://nombresdedominio.cl, Santiago de Chile 2002. Brasil.

[17] RODRIGUEZ Sergio, , *Internet y banca electrónica*, Ponencia para despacho Baker & McKenzie. México.Disponible en: http://www.bakernet.com/ecommerce..

para recibir. De la raíz *dek, dock* o doc., nacen varias palabras. Entre ellas el verbo latino *doceo* y de éste el vocablo *documentum* con 3 acepciones primarias:[18]

Aquello con lo que alguien se instruye; aquello que se refiere a la enseñanza; aquello que se enseña. Por lo tanto se concluye que significa: enseñar.

Y la expresión instrumento, deriva del verbo latino *Instruerer,* es algo que está destinado a instruir e informar acerca del pasado. Si bien parece que hay poca diferencia entre el significado de una y otra expresión, según Pelosi (2001), la expresión Instrumento es más expresiva cuando se quiere hablar de Prueba.

(Giannantonio 2002) distingue entre: Documento Electrónico, en sentido estricto: cuya característica común es que no pueden ser leídos o conocidos por el hombre, sino como consecuencia de la intervención de adecuadas máquinas traductoras que hacen perceptibles y comprensibles las señales digitales (magnéticas) de que están constituidos, los datos están en el mismo ordenador; que es ininteligible para el operador; en otras palabras documento es el archivo electrónico en sí mismo, es decir, un grupo de bits (números binarios ceros y unos-) que en su conjunto representan los caracteres que integran el documento y que podría encontrarse físicamente alojado en un soporte magnético (discos rígidos, unidades de disquetes, cintas de almacenamiento, zips., cd.-room.,) pudiendo ser visualizado o impreso a través de algún periférico de una PC. Y en sentido amplio: es el documento gestado con intervención de un ordenador; en este sentido, es el formado por la computadora a través de sus propios órganos de salida (monitor, impresora), cuya característica es que son perceptibles, y en el caso de textos alfanuméricos, legibles directamente por el hombre sin necesidad de intervenciones por parte de máquinas traductoras.

Los documentos informáticos nacen con la creación de las primeras computadoras pues se llaman documentos informáticos a toda expresión en lenguaje natural o imagen

[18] HAVEY Edwin R., , *Derechos de Autor, de la Cultura y de la Información.* Buenos Aires - Argentina: Editorial Depalma, Biblioteca Personal. 1999.

que sea resultado u obtenida mediante medios informáticos, los primeros documentos fueron dados por las computadoras en los cálculos que hacían, algunas máquinas por su modo de funcionar utilizaban tarjetas que pueden ser consideradas como documentos que calculaban otros documentos.([19])

El documento electrónico debe entenderse como toda expresión en lenguaje natural o convencional y cualquier otra expresión gráfica, sonora o en imagen, recogidas en cualquier tipo de soporte material, incluso los soportes informáticos, con eficacia probatoria o cualquier otro tipo de relevancia jurídica.

2.3. DEFINICIÓN DE DERECHO PENAL

Derecho Penal es: "El conjunto de normas jurídicas de derecho público interno, que define los delitos y señala las penas y medidas de seguridad para lograr la permanencia del orden social".[20]

El criminalista español Eugenio Cuello Calón (2004) lo define como el conjunto de normas que determinan los delitos, las penas que el Estado impone a los delincuentes y a las medidas de seguridad que el mismo establece para la prevención de la criminalidad.

Algunos de los autores distinguen al Derecho Penal, al definirlo entre derecho Penal Subjetivo y Derecho Penal Objetivo. El Derecho Penal en sentido objetivo, dice Cuello Calón (2004), es el conjunto de normas jurídicas establecidas por el Estado que determinan los delitos, las penas y las medidas de seguridad con que aquellos son sancionados.

En México Raúl Carrancá y Trujillo (2002) estima que el derecho objetivamente considerado, es el conjunto de leyes mediante las cuales el Estado define los delitos,

[19] HARVEY, Edwin R, *Derechos de Autor, de la Cultura y de la Información.* Buenos Aires - Argentina: Editorial Depalma, Biblioteca Personal. 1999.
[20] CABANELLAS, Guillermo, *Diccionario Jurídico Elemental. "Derecho Penal"*, Buenos Aires – Argentina. 2000.

determina las penas impunibles a los delincuentes y regula la aplicación concreta de las mismas a los casos de incriminación.

Ignacio Villalobos, en su obra *Derecho Penal Mexicano*, (2001) define al Derecho Penal como "aquella rama del Derecho Público Interno, cuyas disposiciones tienden a mantener el orden político-social de una comunidad, combatiendo por medio de penas y otras medidas adecuadas aquellas conductas que le dañan o ponen en peligro.

El Derecho Penal en sentido subjetivo, consiste en la facultad del Estado para determinar los casos en que deben de imponerse las penas y las medidas de seguridad. Es por esto que para Cuello Calón es el derecho del Estado a determinar, imponer y ejecutar las penas y demás medidas de lucha contra la criminalidad; es el atributo de la soberanía por el cual a todo Estado corresponde reprimir los delitos por medio de las penas; en tanto que objetivamente se forma por el conjunto de normas y de disposiciones que reglamentan el ejercicio de ese atributo: el Estado, como organización política de la Sociedad, tiene como fines primordiales la creación y el mantenimiento del orden jurídico; por tanto, su esencia misma supone el uso de los medios adecuados para tal fin.

2.4. TEORÍA DEL DELITO

La teoría del delito es un sistema de categorización por niveles, conformado por el estudio de los presupuestos jurídico–penales de carácter general que deben concurrir para establecer la existencia de un delito, es decir, permite resolver cuando un hecho es calificable de delito.

Esta teoría, creación de la doctrina (pero basada en ciertos preceptos legales), no se ocupa de los elementos o requisitos específicos de un delito en particular (homicidio, robo, violación, etc.), sino de los elementos o condiciones básicas y comunes a todos los delitos.

Históricamente, se puede hablar de dos corrientes o líneas: la *teoría causalista del delito* y la *teoría finalista del delito*. Para la explicación *causal* del delito la acción es un

movimiento voluntario físico o mecánico, que produce un resultado, el cual es tomado por el tipo penal, sin tener en cuenta la finalidad de tal conducta. La teoría *finalista* del delito, entiende la conducta como un hacer voluntario final, en cuyo análisis debe considerarse los aspectos referidos a la manifestación exterior de esa finalidad. La primera corriente considera, preponderantemente, los elementos referidos al disvalor del resultado; la segunda, por el contrario, pone mayor énfasis, en el disvalor de la acción. Más recientemente, la *teoría funcionalista* intenta constituir un punto de encuentro entre finalistas y causalitas, destacando en esta línea Claus Roxin en Alemania y Paz de la Cuesta en España, entre otros.

La mayoría de los países de la tradición jurídica de Derecho continental, utilizan la teoría finalista del delito. A partir de los años 90, en Alemania, Italia y España, aunque parece imponerse en la doctrina y jurisprudencia la estructura finalista del concepto de delito, se ha iniciado el abandono del concepto de injusto personal, propio de la teoría finalista, para introducirse paulatinamente las aportaciones político-criminales de un concepto funcionalista del delito orientado a sus consecuencias. Quizá la aportación más significativa a la teoría de delito del funcionalismo moderado sea la denominada "Teoría de la imputación objetiva" que introduce el concepto de "riesgo" en la tipicidad, buscado la moderación, en unos casos, de la amplitud de las conductas inicialmente susceptibles de ser consideradas como causa y en otros, la fundamentación de la tipicidad en base a criterios normativos en aquellos supuestos en los que ésta no puede fundamentarse en la causalidad (como sucede en los delitos de omisión, algunas modalidades de delitos de peligro, entre otros).([21])

2.5. CONCEPTO, TIPIFICACIÓN Y CLASIFICACIÓN DE LOS DELITOS INFORMÁTICOS

Constantemente se hace referencia de los beneficios que los medios de comunicación y el uso de la informática han aportado a la sociedad actual, pero la

[21] DE LA CUESTA AGUADO, Paz M. (1995). Tirant lo Blanch (ed.). Tipicidad e Imputación Objetiva, Primera edición;

presente investigación tiene como objeto el estudio de las conductas delictivas que puede generar el gran avance tecnológico, sobre todo en el campo de la informática.

El desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo, porque ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar. Los sistemas de computadoras ofrecen oportunidades nuevas y sumamente complicadas de infringir la ley y han creado la posibilidad de cometer delitos de tipo tradicional en formas no tradicionales.

En los últimos tiempos, ha sido evidente que la sociedad ha utilizado, de manera benéfica, los avances derivados de la tecnología en diversas actividades; sin embargo, es necesario que se atiendan y regulen las cada vez más frecuentes consecuencias del uso indebido de las computadoras y los sistemas informáticos en general. Los llamados *delitos informáticos* no son cometidos por la computadora, sino que es el hombre quien los comete con ayuda de aquella.[22]

En ese entendido, el presente capítulo se dirige al análisis de las posibles medidas preventivas, ya sean de carácter administrativo o penal, que consideramos deben ser tomadas en cuenta para evitar que la comisión de este tipo de infracciones o delitos, alcance en Bolivia los niveles de peligrosidad que se han dado en otros países.

Al iniciar nuestro trabajo, encontramos que no existe un consenso en cuanto al concepto de delito informático, y que estudiosos del tema lo han definido desde diferentes puntos de vista como son el criminógeno, formal, típico y atípico, etc.; dando lugar a que la denominación de que esta conducta haya sufrido diferentes interpretaciones, las que hemos recogido en la primera parte de la investigación. Además, hemos señalado los sujetos, activos, pasivos, clasificación y los tipos de delitos informáticos considerados tanto en la doctrina como en la legislación de diferentes países.([23])

[22] RICARDO Levene, y ALICIA Chiavalloti; "Delitos Informáticos". VI Congreso Iberoamericano Derecho e informática.
[23] SARZANA, Carlos en su obra "Criminalitá e tecnología, los crímenes por computadora "Cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, o como mero símbolo".

2.5.1. Concepto de Delitos Informáticos

El delito informático implica actividades criminales que en un primer momento los países han tratado de encuadrar características típicas de carácter tradicional, tales como *robos, hurtos, fraudes, falsificaciones, perjuicios, estafa, sabotaje,* etc. Sin embargo, debe destacarse que el uso de las técnicas informáticas ha creado nuevas posibilidades del uso indebido de las computadoras lo que ha propiciado, a su vez, la necesidad de regulación por parte del derecho.

A nivel internacional se considera que no existe una definición propia del delito informático, sin embargo muchos han sido los esfuerzos de expertos que se han ocupado del tema, y aún cuando no existe una definición con carácter universal, se han formulado conceptos funcionales atendiendo a realidades nacionales concretas.([24])

Por lo que se refiere a las definiciones que se han intentado dar, cabe destacar que Julio Téllez Valdés señala que no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación especial, ya que para hablar de *delitos* en el sentido de acciones típicas, es decir, tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión *delitos informáticos* esté consignada en los códigos penales, lo cual en nuestro país, al igual que en muchos otros, cuenta con una regulación en el capítulo XI artículos 363 bis y 363 ter, ésta es absolutamente general y adolece de vacíos jurídicos.

Para *Carlos Sarzana,* en su obra Criminalista e tecnología, los crímenes por computadora comprenden cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material u objeto de la acción criminógena y como un mero símbolo.

[24] GUIBOURG, Ricardo. "Manual de informática jurídica". Astrea - Correa. "Derecho informático". Depalma.

Nidia Callegari define el delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".([25])

Rafael Fernández Calvo define el 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 1 de la constitución española".([26])

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

Téllez, conceptualiza el delito informático en forma típica y atípica, entendiendo la primera como "las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" y por la segunda "actitudes ilícitas en que se tienen a las computadoras como instrumento o fin".([27])

Por otra parte, debe mencionarse que se han formulado diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora, tales como *delitos informáticos*, *delitos electrónicos*, *delitos relacionados con las computadoras*, *crímenes por computadora*, "delincuencia relacionada con el ordenador".([28])

En este orden de ideas, en el presente trabajo se entenderá como *delitos informáticos* todas aquellas conductas ilícitas susceptibles de ser sancionadas por el

[25] Citado por: Nuñez Ponce, Julio. "Derecho informático". Marsol Pérez Luño, Antonio. "Manual de informática y derecho". Ariel Derecho.
[26] Citado por: Jijena Leiva, Renato Javier: "La Criminalidad Informática": Situación de Lege Data y Lege Ferenda en Chile". Actas de III Congreso Iberoamericano de Informática y Derecho". Mérida, España.
[27] Citado por: Luis Alberto VIERA - "La prueba", en A.A.V.V. - "Curso de Derecho Procesal" (Facultad de Derecho y C.S., Montevideo, 1974), tomo II, pág. 117 y sgtes. Abogados Derecho Informático - http://www.iurisdata.com Despacho de abogados especializado en derecho informático y telecomunicaciones: comercio electrónico, marketing on-line, propiedad intelectual, etc.
[28] PUCCETTI, Doris Liliana. Revista Notarial. Colegio de Escribanos de la Provincia de Córdoba. Año 1999-1- Nº 77. "El documento electrónico" Pág. 85 a 91.

derecho penal, que hacen uso indebido de cualquier medio informático, este concepto no abarca las infracciones administrativas que constituyen la generalidad de las conductas ilícitas presentes por ejemplo en México debido a que la legislación se refiere al derecho de autor y propiedad intelectual, sin embargo, se deberá tener presente que la propuesta final de este trabajo tiene por objeto la regulación penal de aquellas actitudes antijurídicas que estimamos más graves como último recurso para evitar su impunidad.

2.6. EL DELINCUENTE INFORMÁTICO Y SUS CARACTERÍSTICAS CRIMINOLÓGICAS

Son auténticos genios de la informática, entran sin permiso en ordenadores y redes ajenas, husmean, rastrean y en ocasiones, dejan sus peculiares tarjetas de visita. Los Hackers posmodernos corsarios de la red, son el último avance de la delincuencia informática en este de siglo.

Parecen más bien una pandilla que se divierte haciendo travesuras. El hecho de hacer girar por los aires las encriptadas claves de acceso de los ordenadores más *seguros* del mundo, entrar en las redes de información de gobiernos y organismos oficiales, y simplemente, echar un vistazo y salir dejando una pequeña *tarjeta de visita*[29], parece suficiente para estos corsarios posmodernos no roban, matan, ni destrozan, simplemente observan.

En 1996 *observadores informáticos* accedieron 162.586 veces a las bases de datos estadounidenses, que presumen ser las más protegidas del planeta.

Mitnik quien con sólo 16 años fue un pionero, impuso su lema *"La información es pública, es de todos y nadie tiene derecho a ocultarla"* y cuando fue detenido sostuvo que no se creía un delincuente y decía *"Un Hacker es sólo un curioso, un investigador, y aquí*

[29] Se entiende por tarjeta de visita al modo o manera peculiar en que el visitante clandestino o no autorizado deja un mensaje para que los usuarios o quienes tengan la contraseña sepan de su visita.

vuestra intención equivale a enviar a un descubridor a la hoguera, como lo hacía la inquisición".[30]

Lo que está claro es que, mientras los *cibercorsarios* mejoran sus esfuerzos por hacer saltar los sistemas de seguridad de los computadores más controlados, las compañías desarrollan mecanismos de protección más sofisticados. En el *Jargón File* se ha publicado un compendio comprensivo del Hacker que comprende su tradición, folklore y humor.

Este documento es una colección de términos utilizados en la *Subcultura del Hacker* aunque en él se incluyen términos técnicos, se intenta describir el modus vivendi del Hacker, en el que tendrá valores compartidos, sus propios mitos, héroes, diversiones, tabúes, sueños, hábitos, etc.

Esta Subcultura nació, aproximadamente, hace cuarenta años compuesta por personas particularmente creadoras y, como en toda Subcultura el vocabulario particular del Hacker, ha contribuido al sostenimiento de su cultura, además de ser utilizado por un lado como una herramienta de comunicación, por otro de inclusión y de exclusión. Son conscientes e inventivos en el uso del idioma, rasgos que parecen ser comunes en niños y jóvenes.

Se denomina a la Subcultura del Hacker como ***hacker down*** y su intención es extenderse prefiriendo calidad más que cantidad. Según los subculturalistas se podría definir al Hacker down como un nuevo tipo de subcultura con un factor criminógeno latente. Opinan que las pandillas, lejos de hallarse desorganizadas, se encuentran sujetas a un sistema de valores, normas y conductas compartidas que constituyen su propia cultura; claro está que la subcultura no coincide con los valores y normas centrales u oficiales, más bien constituye una suerte de sociedad de recambio.

[30] LEVENE, Ricardo y CHIAVALLOTI, Alicia. "Delitos Informáticos". VI Congreso Iberoamericano Derecho e informática.

Cohen acentúa el hecho de que la delincuencia subcultural no aparece como una dinámica antisocial, sino *disocial*, donde el grupo tiene su sistema de valores, sus propias normas, sus formas de *Status* y sus reglas de prestigio. Se podría decir, en términos conductistas, que los miembros de grupo tienen sus propios impulsos, sus modelos, refuerzos y modos de satisfacerlos, además gozan de la aprobación del grupo, ello refuerza la conducta criminógena.

A diferencia de las personalidades antisociales, los delincuentes Subculturales (*dissocial)* pueden desarrollar lazos interpersonales genuinos, compartiendo un continuado y significativo aprendizaje de evitación (de la detección o de la condena).

2.6.1. El Hacker

Es una persona muy interesada en el funcionamiento de sistemas operativos; aquel curioso que simplemente le gusta husmear por todas partes, llegar a conocer el funcionamiento de cualquier sistema informático mejor que quiénes lo inventaron. Esta palabra es un término en ingles que caracteriza al delincuente silencioso o tecnológico. Ellos son capaces de crear su propio software para entrar a los sistemas. Toma su actividad como un reto intelectual, no pretende producir daños e incluso se apoya en un código ético.([31])

- El acceso a los ordenadores y a cualquier cosa que le pueda enseñar cómo funciona el mundo, a su vez debería ser limitado y total.
- Toda la información deberá ser libre y gratuita.
- Desconfía de la autoridad, promueve la descentralización.
- Los Hackers deberán ser juzgados por sus hacks, no por criterios sin sentido como calificaciones académicas, edad, raza, o posición social.
- Se puede crear arte y belleza en un ordenador.
- Los ordenadores pueden mejorar la vida de las personas.

[31] Ver: SILVA Neto, Amaro Morales. Rescatemos los hackers. Disponible en www.jus.com.br/ doutrina/hackers.html

La visión que se tiene de ellos no se ajusta a la realidad, ya que hay una fina línea entre actuar así y producir un daño o caer en la tentación de robar información. Por no mencionar que en numerosas legislaciones, el solo hecho de colocarse en un sistema ya es un delito. A pesar de ello, hay quienes opinan que el acceso a sí mismo a un sistema, no puede ser considerado a priori como delito, sino se dan los requisitos, objetivos y subjetivos que configuran los tipos penales correspondientes.([32])

El hacking propiamente dicho, según este autor, es un delito informático que consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información, con el fin de obtener una satisfacción de carácter intelectual por el desciframiento de los códigos de acceso o password, no causando daños inmediatos y tangibles en la victima, o bien por la mera voluntad de curiosear o divertirse de su autor. La voluntad de divertirse generalmente se traduce por paseos por el sistema haciendo alarde de su intromisión. Es lo que se ha llamado JOY RIDING O PASEOS DE DIVERSIÓN.[33]

Las características de esta clase de hacking son las siguientes: el Hacker es una persona experta en materias informáticas y con edad fluctuante entre los 15 y 25 años, es por ello que a esta delincuencia se ha denominado *SHORT PANTS CRIMES*, es decir, en pantalones cortos, su motivación no es la de causar daño, sino de obtener personales satisfacciones y orgullos, basados principalmente en la burla de los sistemas de seguridad dispuestos.

2.6.2. El Cracker

Personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas. El Pirata informático tiene dos variantes:

[32] REGLAMENTO DEL SOPORTE LÓGICO O SOFTWARE; Jurisprudencia Argentina.-Tomo II- Año 1999- "Documento Electrónico" por Daniel Altmark, págs. 851-855.
[33] Derecho de la Informática - http://members.xoom.com/asacer/Derecho/indice.htm Breve introducción a la ley aplicada a la informática.

- El que penetra en un sistema informático y roba información o se produce destrozos en el mismo.
- El que se dedica a desproteger todo tipo de programas, tanto de versiones shareware para hacerlas plenamente operativas como de programas completos comerciales que presentan protecciones anti-copia.
- Cracker es aquel Hacker fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas.

Para los grandes fabricantes de sistemas y la prensa este grupo es el más rebelde de todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica ahí, sino en que esta rotura es difundida normalmente a través de la Red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers.([34])

Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware. Así, es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto equivale a la parte de programación y la parte física de la electrónica. Como su nombre indica se dedican a romper, por supuesto las protecciones y otros elementos de seguridad de los programas comerciales, con el fin confeso de sacar provecho de los mismos.

2.6.3. El Phreaker

Es el especialista en telefonía (Cracker de teléfono). Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles. En la actualidad poseen conocimientos de tarjetas prepago, ya que la telefonía celular las emplea habitualmente. Sin embargo, es en estos últimos días, cuando un buen Phreaker debe tener amplios conocimientos sobre informática, puesto que la telefonía celular o el control de centralitas es la parte primordial a tener en cuenta y/o emplean la informática para su procesado de datos.

[34] Datum Lex, Privacidad y Protección de Datos - http://www.datumlex.com
Web jurídica dedicada a la información y legislación sobre privacidad y protección de datos, criptografía, anonimato y hacktivismo en redes informáticas. Noticias diarias y boletines gratuitos.

Éstos buscan burlar la protección de las redes públicas y corporativas de telefonía, con el fin de poner a prueba conocimientos y habilidades (en la actualidad casi todas estas redes de comunicaciones son soportadas y administradas desde sistemas de computación), pero también el de obviar la obligatoriedad del pago por servicio, e incluso lucrar con las reproducciones fraudulentas de tarjetas de prepago para llamadas telefónicas, cuyos códigos se obtienen al lograr el acceso mediante técnicas de *Hacking* a sus servidores.([35])

Dentro de las actuales manifestaciones de phreaking podríamos distinguir:

- **Shoulder–surfing**

  Esta conducta se realiza por el agente mediante la observación del código secreto de acceso telefónico que pertenece a su potencial víctima, el cual lo obtiene al momento en que ella lo utiliza, sin que la víctima pueda percatarse de que está siendo observada por este sujeto quien, posteriormente, aprovechará esa información para beneficiarse con el uso del servicio telefónico ajeno. ([36]).

- **Call-sell operations**

  El accionar del sujeto activo consiste en presentar un código identificador de usuario que no le pertenece y carga el costo de la llamada a la cuenta de la víctima. Esta acción aprovecha la especial vulnerabilidad de los teléfonos celulares y principalmente ha sido aprovechada a nivel internacional por los traficantes de drogas.

- **Diverting**

  Consiste en la penetración ilícita a centrales telefónicas privadas, utilizando éstas para la realización de llamadas de larga distancia que se cargan

[35] Delitos Informáticos -- SEGURIDAD, CIFRADO Y FIRMA ELECTRÓNICA
Que "el que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u www.delitosinformaticos.com/seguridad/firma.shtml

[36] JIJENA LEIVA, Renato Javier: "La Criminalidad Informática": Situación de Lege Data y Lege Ferenda en Chile". Actas de III Congreso Iberoamericano de Informática y Derecho". Mérida, España.

posteriormente al dueño de la central a la que se ingresó clandestinamente. La conducta se realiza atacando a empresas que registren un alto volumen de tráfico de llamadas telefónicas, con el fin de hacer más difícil su detección. ([37])

- **Acceso no autorizado a sistemas de correos de voz**

  El agente ataca por esta vía las máquinas destinadas a realizar el almacenamiento de mensajes telefónicos destinados al conocimiento exclusivo de los usuarios suscriptores del servicio. A través de esta conducta el sujeto activo puede perseguir diversos objetivos:

  - Utilizar los códigos de transferencia de mensajería automática manejados por el sistema.
  - Lograr el conocimiento ilícito de la información recibida y grabada por el sistema.
  - Monitoreo pasivo por medio de esta conducta el agente intercepta ondas radiales para tener acceso a información transmitida por las frecuencias utilizadas por los teléfonos inalámbricos y los celulares. ([38])

    En nuestro país actúan de forma más restringida pues el servicio no está plenamente generalizado por lo que las posibilidades de acceso a estos sistemas son más esporádicas que en otros países, divergiendo esto del riesgo; más los comisores no desaparecen, sólo disminuyen en cantidad. Posteriormente haremos mención en este capítulo referente a la forma en que se manifiestan esta actitud delictiva, analizando a fondo la proyección de estos.

2.6.4. Trashing

Esta conducta tiene la particularidad de haber sido considerada recientemente en relación con los delitos informáticos. Apunta a la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura (material o inmaterial)

[37] bis idem.
[38] In bis idem.

descartada por una persona, una empresa u otra entidad, con el fin de utilizarla por medios informáticos en actividades delictivas. Estas acciones corresponden a una desviación del procedimiento conocido como reingeniería social.

Estas actividades pueden tener como objetivo la realización de espionaje, coerción o simplemente el lucro mediante el uso ilegítimo de códigos de ingreso a sistemas informáticos que se hayan obtenido en el análisis de la basura recolectada. Esta minuciosa distinción de sujetos según su actuar no son útiles para tipificar el delito pues son sujetos indeterminados, no requieren condición especial; más vale realizar dicha diferenciación para ubicarnos en el marco en que se desenvuelven y las características de su actuar, favoreciendo con ello el procedimiento penal que se deberá llevar a cabo luego de producirse el delito.([39])

La gran mayoría de los hackers, en sentido general, copian herramientas que desarrollaron otros. Actualmente, existen alrededor de 60 mil páginas que explican con todo detalle muchos de los trucos para piratear. Sólo basta con bajar un programa y comenzar a bombardear un sitio para lograr las primeras experiencias. Incluso, hay algunas páginas que ofrecen laboratorios de virus, donde la persona puede crearlos a su medida, siguiendo instrucciones básicas. Además por medio de estos programas van aprendiendo a desarrollar sus propias herramientas.

Entre los métodos preferidos por estos delincuentes para desarrollar su actuar son:

- Puertas falsas: puertas de entrada "que sirven para hacer la revisión o la recuperación de información en caso de errores en el sistema Consiste en aprovechar los accesos".
- Llave maestra (superzapping): El uso no autorizado de programas para modificar, destruir, copiar, insertar, utilizar o impedir el uso de datos archivados en un sistema informático. El nombre proviene de un programa de

[39] **HAWKRIDG**E, David. Informática y Educación. las nuevas tecnologías de la información. Ed. Abeledo- Perrot. Buenos. Aires Argentina, 1992.

utilidad que se llama superzap, que permite abrir cualquier archivo de una computadora aunque se halle protegido por medidas de seguridad.

- Pinchado de líneas: Se realiza a través de la interferencia de las líneas telefónicas o telemáticas a través de las cuales se transmiten las informaciones procesadas en las bases de datos informáticas. ([40])

Un aspecto a diferenciar entre un hacker y un cracker puede ser que el primero crea sus propios programas, ya que tiene muchos conocimientos en programación, y además en varios lenguajes de programación, mientras que el Segundo se basa en programas ya creados que puede adquirir normalmente, vía Internet.

Otro aspecto lo es que el interés de un cracker es destrozar la máquina que hay al otro lado, vender información al mejor postor, destruyen datos, modifican ficheros, introducen en los programas códigos malignos que crean problemas en el sistema donde se ejecutan, o sea, lo único que hacen es crear problemas en la red; no es constructivo como un hacker, que trata de mejorar la red dando a conocer sus incursiones y los fallos que ha encontrado.([41])

El sujeto pasivo seguirá siendo la víctima del delito, el propietario legítimo del bien jurídico protegido, sobre quien recae la conducta de acción u omisión que realiza el sujeto activo. En el caso de estos delitos los sujetos pueden ser persona natural o jurídica que usan sistemas automatizados de información, generalmente conectados a otros. Mediante el sujeto pasivo podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, aunque estos generalmente no son descubiertos o no son denunciados a las autoridades responsables; tal vez la razón de ello es la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y aplicar el tratamiento jurídico adecuado a esta problemática; o bien el temor a su empresa y las consecuentes pérdidas económicas; u otros motivos.

[40] In bis Idem
[41] In bis Idem.

2.7. SUJETO ACTIVO EN LOS DELITOS INFORMÁTICOS

Las personas que cometen los *Delitos Informáticos* son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.([42])

Con el tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y que lo que los diferencia entre sí es la naturaleza de los cometidos. De esta forma, la persona que entra en un sistema informático sin intenciones delictivas es muy diferente del empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.

El nivel típico de aptitudes del delincuente es tema de controversia ya que para algunos en el nivel de aptitudes no es indicador de delincuencia informática en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Sin embargo, teniendo en cuenta las características ya mencionadas de las personas que cometen los *delitos informáticos*, estudiosos en la materia los han catalogado como *delitos de cuello blanco* término introducido por primera vez por el criminológico norteamericano Edwin Sutherland en el año de 1943.

Efectivamente, este conocido criminólogo señala un sinnúmero de conductas que considera como *delitos de cuello blanco*, aun cuando muchas de estas conductas no están tipificadas en los ordenamientos jurídicos como delitos, y dentro de las cuales cabe

[42] In Bis Idem.

destacar las violaciones a las leyes de patentes y fábrica de derechos, el mercado negro, el contrabando en las empresas, la evasión de impuestos, las quiebras fraudulentas, corrupción de altos funcionarios entre otros.

Asimismo, este criminológico estadounidense dice que tanto la definición de los *delitos informáticos* como las de los *delitos de cuello blanco* no es de acuerdo al interés protegido, como sucede en los delitos convencionales sino de acuerdo al sujeto activo que los comete. Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

Hay dificultad para elaborar estadísticas sobre ambos tipos de delitos. La *cifra negra* es muy alta; hay dificultades para descubrirlo y sancionarlo, en razón del poder económico de quienes los cometen, pero los daños económicos son altísimos; existe una gran indiferencia de la opinión pública sobre los daños ocasionados a la sociedad; la sociedad no considera delincuentes a los sujetos que cometen este tipo de delitos, no los segrega, no los desprecia, ni los desvaloriza, por el contrario, el autor o autores de este tipo de delitos se considera a sí mismos *respetables* otra coincidencia que tiene estos tipos de delitos es que, generalmente, son objeto de medidas o sanciones de carácter administrativo y no privativos de la libertad.

2.8. SUJETO PASIVO DE LOS DELITOS INFORMÁTICOS

En primer término tenemos que distinguir que sujeto pasivo o 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.

El sujeto pasivo del delito que nos ocupa, es sumamente importante para el estudio de los *delitos informáticos*, ya que mediante él podemos conocer los diferentes ilícitos

que cometen los delincuentes informáticos, con 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.([43])

Dado lo anterior, "ha sido imposible conocer la verdadera magnitud de los *delitos informáticos*, ya que la mayor parte de los delitos no son descubierto o no son denunciados a las autoridades responsables"([44]) y si a esto se suma la falta de leyes que protejan a las víctimas de estos delitos; la falta de preparación por parte de las autoridades para comprender, investigar y dar tratamiento jurídico adecuado a esta problemática; el temor por parte de las empresas de denunciar este tipo de ilícitos por el desprestigio que esto pudiera ocasionar a su empresa y las consecuentes pérdidas económicas, entre otros más, trae como consecuencia que las estadísticas sobre este tipo de conductas se mantenga bajo la llamada *cifra oculta o cifra negra.*

Por lo anterior, se reconoce que para conseguir una prevención efectiva de la criminalidad informática se requiere, en primer lugar, un análisis objetivo de las necesidades de protección y de las fuentes de peligro. Una protección eficaz contra la criminalidad informática presupone ante todo que las víctimas potenciales conozcan las correspondientes técnicas de manipulación, así como sus formas de encubrimiento.

En el mismo sentido, se puede decir que mediante la divulgación de las posibles conductas ilícitas derivadas del uso de las computadoras, y alertando a las potenciales víctimas para que tomen las medidas pertinentes a fin de prevenir la delincuencia informática, y si a esto se suma la creación de una adecuada legislación que proteja los intereses de las víctimas y una eficiente preparación por parte del personal encargado de la procuración, administración y la impartición de justicia para atender e investigar estas conductas ilícitas, se estaría avanzando mucho en el camino de la lucha contra la delincuencia informática, que cada día tiende a expandirse más.

---

[43] LEVENE, Ricardo y CHIAVALLOTI, Alicia. "Delitos Informáticos". VI Congreso Iberoamericano Derecho e informática.
[44] TELLEZ Valdez, Julio. "Derecho Informático", Ed. Mc. Graw - Hill México. 1997 p. 56 y 70.

Además, se debe destacar que los organismos internacionales han adoptado resoluciones similares en el sentido de que "educando a la comunidad de víctimas y estimulando la denuncia de los delitos se promovería la confianza pública en la capacidad de los encargados de hacer cumplir la ley y de las autoridades judiciales para detectar, investigar y prevenir los delitos informáticos".([45])

2.9. CLASIFICACIÓN DE DELITOS INFORMÁTICOS

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

- **Como medio y objetivo:**

En esta categoría se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física.

María de la Luz Lima, presenta una clasificación, de lo que ella llama *delitos electrónicos*, diciendo que existen tres categorías, a saber:

- Los que utilizan la tecnología electrónica como método;
- Los que utilizan la tecnología electrónica como medio; y
- Los que utilizan la tecnología electrónica como fin.

- **Como método**

Conductas criminales en donde los individuos utilizan métodos electrónicos para llegar a un resultado ilícito.

- **Como objeto**

Es cuando se alteran datos de documentos que se encuentran almacenados en forma computarizada. Pueden falsificarse o adulterarse también micro formas, micro duplicados

[45] TELLEZ Valdez, Julio; "Derecho Informático", Ed. Mc. Graw - Hill México. 1997 p.56-70.

y microcopias; esto puede llevarse a cabo en el proceso de copiado o en cualquier otro momento.

- **Como instrumentos**

Las computadoras pueden utilizarse para realizar falsificaciones de documentos de uso comercial. Las fotocopiadoras computarizadas en color a base de rayos láser dieron lugar a nuevas falsificaciones. Estas fotocopiadoras pueden hacer copias de alta resolución, modificar documentos, crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que solo un experto puede diferenciarlos de los documentos auténticos.([46])

- **Como medio**

Son conductas criminógenas en donde para realizar un delito utilizan una computadora, como medio o símbolo.

- **Como instrumento o medio.**

En esta categoría se encuentran las conductas criminales que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito, por ejemplo:

- Falsificación de documentos vía computarizada (tarjetas de crédito, cheques, etc.).
- Variación de los activos y pasivos en la situación contable de las empresas.
- Planeamiento y simulación de delitos convencionales (robo, homicidio, fraude, etc.).
- Lectura, sustracción o copiado de información confidencial.
- Modificación de datos tanto en la entrada como en la salida.
- Aprovechamiento indebido o violación de un código para penetrar a un sistema introduciendo instrucciones inapropiadas.

[46] Consultar: Davara & Davara Asesores Jurídicos Documentos Relacionados: Protección de Datos; Comercio electrónico; Protección de los. Pago-ey TEF; Propiedad Intelectual e Industrial; Contratos informáticos; www.davara.com/documentos/relacionados.

- Variación en cuanto al destino de pequeñas cantidades de dinero hacia una cuenta bancaria apócrifa.
- Uso no autorizado de programas de cómputo.
- Introducción de instrucciones que provocan *interrupciones* en la lógica interna de los programas.
- Alteración en el funcionamiento de los sistemas, a través de los virus informáticos.
- Obtención de información residual impresa en papel luego de la ejecución de trabajos.
- Acceso a áreas informatizadas en forma no autorizada.
- Intervención en las líneas de comunicación de datos o teleproceso.

- **Como fin**

Conductas criminógenas dirigidas contra la entidad física del objeto o máquina electrónica o su material con objeto de dañarla.

- **Como fin u objetivo**

En esta categoría, se enmarcan las conductas criminales que van dirigidas contra las computadoras, accesorios o programas como entidad física, como por ejemplo:

- Programación de instrucciones que producen un bloqueo total al sistema.
- Destrucción de programas por cualquier método.
- Daño a la memoria.
- Atentado físico contra la máquina o sus accesorios.
- Sabotaje político o terrorismo en que se destruya o surja un apoderamiento de los centros neurálgicos computarizados.
- Secuestro de soportes magnéticos entre los que figure información valiosa con fines de chantaje (pago de rescate, etc.).

- Por otra parte, existen diversos tipos de delito que pueden ser cometidos y que se encuentran ligados directamente a acciones efectuadas contra los propios sistemas como son:[47]
    - **Acceso no autorizado:** Uso ilegitimo de passwords y la entrada de un sistema informático sin la autorización del propietario.
    - **Destrucción de datos:** Los daños causados en la red mediante la introducción de virus, bombas lógicas, etc.
    - **Infracción al copyright de bases de datos:** Uso no autorizado de información almacenada en una base de datos.
    - **Interceptación de e-mail:** Lectura de un mensaje electrónico ajeno.
    - **Estafas electrónicas:** A través de compras realizadas haciendo uso de la red.
    - **Transferencias de fondos:** Engaños en la realización de este tipo de transacciones.
    - Por otro lado, la red Internet permite dar soporte para la comisión de otro tipo de delitos:
    - **Espionaje:** Acceso no autorizado a sistemas informáticos gubernamentales y de grandes empresas e interceptación de correos electrónicos.
    - **Terrorismo:** Mensajes anónimos aprovechados por grupos terroristas para remitirse consignas y planes de actuación a nivel internacional.
    - **Narcotráfico:** Transmisión de fórmulas para la fabricación de estupefacientes, para el blanqueo de dinero y para la coordinación de entregas y recogidas.
    - **Otros delitos:** Las mismas ventajas que encuentran en la Internet los narcotraficantes pueden ser aprovechadas para la planificación de otros delitos como el tráfico de armas, proselitismo de sectas, propaganda de grupos extremistas, y cualquier otro delito que pueda ser trasladado de la vida real al ciberespacio o al revés.

[47] **GIRALDO**, Jaime. ***Informática Jurídica Documental***. Temis. Colombia. 1.990. Pág. 192.

Al respecto, según un estudio publicado en el Manual de las Naciones Unidas en la prevención y control de delitos informáticos (N° 43 y 44), el 90% de los delitos realizados mediante la computadora fueron ejecutados por empleados de la propia empresa afectada. Asimismo, otro reciente estudio realizado en América del Norte y Europa indicó que el 73% de las intrusiones cometidas eran atribuibles a fuentes interiores y solo el 23% a la actividad delictiva externa. El nivel típico de aptitudes del delincuente informático es tema de controversia ya que para algunos el nivel de aptitudes no es indicador de delincuencia informática, en tanto que otros aducen que los posibles delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos.

Entre las características en común que poseen ambos delitos tenemos que: el sujeto activo del delito es una persona de cierto status socioeconómico, su comisión no puede explicarse por pobreza ni por mala habitación, ni por carencia de recreación, ni por baja educación, ni por poca inteligencia, ni por inestabilidad emocional.

2.10. OTROS DELITOS INFORMÁTICOS

En lo que se refiere a delitos informáticos, Olivier Hance en su libro *Leyes y Negocios en Internet,* considera tres categorías de comportamiento que pueden afectar negativamente a los usuarios de los sistemas informáticos. Las mismas son las siguientes:

- **Acceso no autorizado:** Es el primer paso de cualquier delito. Se refiere a un usuario que, sin autorización, se conecta deliberadamente a una red, un servidor o un archivo (por ejemplo, una casilla de correo electrónico), o hace la conexión por accidente pero decide voluntariamente mantenerse conectado.
- **Actos dañinos o circulación de material dañino:** Una vez que se conecta a un servidor, el infractor puede robar archivos, copiarlos o hacer circular información negativa, como virus o gusanos. Tal comportamiento casi siempre

se es clasificado como Piratería (apropiación, descarga y uso de la información sin conocimiento del propietario) o como sabotaje (alteración, modificación o destrucción de datos o de software, uno de cuyos efectos es paralizar la actividad del sistema o del servidor en Internet).

- **Interceptación no autorizada:** En este caso, el hacker detecta pulsos electrónicos transmitidos por una red o una computadora y obtiene información no dirigida a él.

Las leyes estadounidense y canadiense, lo mismo que los sistemas legales de la mayoría de los países europeos, han tipificado y penalizado estos tres tipos de comportamiento ilícito cometidos a través de las computadoras.

Por su parte, el Manual de la Naciones Unidas para la Prevención y Control de Delitos Informáticos señala que cuando el problema se eleva a la escena internacional, se magnifican los inconvenientes y las insuficiencias, por cuanto los delitos informáticos 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 a 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 las 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 de mecanismos sincronizados que permitan la puesta en vigor de la cooperación internacional.

2.11. TIPOS DE DELITOS INFORMÁTICOS

Entre los tipos de delitos informáticos reconocidos por Naciones Unidas se puede citar:

2.11.1. Fraudes cometidos mediante manipulación de computadora

- **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.([48])

- **La manipulación de programas**

Este tipo de delito 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 tiene 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.

[48] Renato, Jijena. *Impunidad y Delito Informático*. Disponible en: http://www.delitosen lared.org, Recuperado el: 16 de marzo de 1996.

- **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 el 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.

En este sentido, es un fraude efectuado por manipulación informática que aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina *técnica de salchichón* en la que rodajas muy finas apenas perceptibles, de transacciones financieras, se van sacando repetidamente de una cuenta y se transfieren a otra.[49]

2.11.2. Falsificaciones informáticas

Las falsificaciones informáticas pueden darse según el uso que se le dé, es así que se puede falsificar:

- **Como objeto**

Ocurre 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

[49] In Idem

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.

2.11.3. Daño o modificación de programas o datos computarizados

- **Sabotaje informático**

Se refiere al acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

- **Virus**

Es una serie de claves programáticas que pueden adherirse a los programas legítimos, y propagarse a otros programas informáticos. Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya.

- **Gusanos**

Se fabrica en forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el virus es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus; por ejemplo, un programa gusano que subsiguientemente se destruirá puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita.([50])

[50] Ver: In bis Idem.

- **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 menciona 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.([51])

- **Reproducción no autorizada de programas informáticos de protección legal**

La reproducción no autorizada de programas informáticos, 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.

2.11.4. Clasificación del delito informático

En general, existen tres clases de comportamiento que afectan a los usuarios de un sistema informático: Acceso no autorizado, actos dañinos o circulación de material dañino e intercepción no autorizada. Otros autores han clasificado a los delitos informáticos en base dos criterios: como ser: como medio o como objetivo. El primero se refiere a las conductas que se valen de las computadoras como método o medio. El segundo se relaciona con las conductas dirigidas en contra de la computadora, accesorios o programas. Por otro lado, Las Naciones Unidas establecen tres tipologías de delitos informáticos:

[51] DA COSTA RODRIGUEZ, Marco Aurelio Rodriguez**. "***Crimes de Informática"*. Revista electrónica Jus Navegando. Disponible en: www.jus.com.br/doutrina/crinfo.html.

- Fraudes cometidos mediante manipulación de computadoras. En cada caso, lo que se trata es de colocar datos falsos en un sistema u obtener los datos del sistema en forma ilegal. Entre estos tenemos: la manipulación de datos de entrada y salida así como la manipulación de programas.
- Falsificaciones Informáticas.
- Utilización de computadoras como instrumento para falsificar (entradas, tickets dinero, etc.).
- Daños a Datos Computarizados.

En general se trata de programas o accionares que dañan la información de un sistema determinado. En este grupo se encuentran los gusanos, accesos no autorizados, los virus, etc. (SARZANA, Carlos: 2009:73).

El Convenio de Ciberdelincuencia del Consejo de Europa firmado en Budapest el 2001 plantea una clasificación de los delitos informáticos en cuatro grupos:

- **Delitos contra la confidencialidad,** la integridad y la disponibilidad de los datos y sistemas informáticos: Acceso ilegal a sistemas informáticos, para la interceptación ilícita de datos informáticos, interferencia en el funcionamiento de un sistema informático, abuso de dispositivos que faciliten la comisión de delitos1.
- **Delitos informáticos:** Falsificación informática por medio de la introducción, borrado o supresión de datos informáticos, Fraude informático mediante la introducción, alteración o borrado de datos informáticos o interferencia en sistemas informáticos.
- **Delitos relacionados con el contenido:** En este grupo se encuentran: la posesión, producción, difusión o adquisición de pornografía infantil, a través de un sistema informático.
- **Delitos relacionados con infracciones de la propiedad intelectual y derechos afines:** En este grupo de delitos se encuentran por ejemplo la piratería informática. (SARZANA, Carlos: 2009:75-78).

2.12. LOS BIENES JURÍDICOS AFECTADOS EN LOS DELITOS INFORMÁTICOS:

A pesar de las discrepancias doctrinales cada vez son más tratadistas que indican la necesidad de creación de una nueva categoría jurídico penal para las conductas vinculadas con el hecho informático, ya que se trata solamente de la lesión de bienes jurídicos tradicionales, sino también de un nuevo interés que debe ser tratado por el Derecho Penal. (Sarzana: 2009:80-81) Sin embargo no existen criterios unificados para definir este interés así como el bien jurídico penal relacionado. Las diferentes posiciones son las siguientes.

- **La Seguridad Informática:** La cada vez, más acelerada ampliación del uso de redes y sistemas informáticos, que son fundamentales para el desarrollo de una sociedad determina que la protección de su seguridad sirva como medio para proteger bienes de carácter individual (intimidad, patrimonio, honor, etc.) así como otros bienes de carácter supraindividual (seguridad del Estado, orden público, etc.). En otras palabras, se trata a la seguridad informática como un bien jurídico colectivo a tutelar para evitar la lesión de una serie de bienes jurídicos de carácter individual. Cuando se afecta un sistema informático determinado no sólo se daña un bien jurídico individual, sino que se generan riesgos para la colectividad de usuarios. Por tanto se trata de un bien jurídico de naturaleza colectiva. (Sarzana: 2009:89-91)

- **La integridad, confidencialidad y disponibilidad de datos y sistemas informáticos:** Trata de proteger la informatización de los datos públicos y privados, para poder confiar en su autenticidad y disponibilidad como una garantía del desarrollo cultural, económico y social. Es considerado un bien jurídico de carácter supraindividual que requiere intervención penal y es instrumental respecto de otros bienes jurídicos que pueden verse dañados por los atentados contra la accesibilidad, integridad o confidencialidad de determinados datos. (Sarzana: 2009: 91).

- **Intimidad informática:** Se entiende que debe protegerse el bien jurídico individual de intimidad e inviolabilidad informáticas. Su contenido fundamental consiste en el derecho del individuo a decidir qué información personal se puede difundir sobre él así como el destino de esta difusión. (Sarzana: 2009:94).
- **Otras concepciones:** Debido a la gran dependencia de la sociedad en relación a la informática para el desarrollo cultural, personal, económico y social, los delitos vinculados con la informática no sólo dañan bienes jurídicos individuales y concretos sino que también ponen en peligro la confianza de la sociedad en el buen funcionamiento de los sistemas informáticos y de las redes de transmisión de datos. Por lo que también se señala como nuevo bien jurídico de carácter supraindividual la confianza en el funcionamiento de los sistemas informatizados. (Sarzana: 2009:105).

2.13. TEORÍA DE SUSTENTO. LA INFORMACIÓN COMO BIEN JURÍDICO INTERMEDIO:

En la presente investigación el análisis se basa en la teoría relativa a la protección del derecho a la información como bien jurídico que resulta afectado con los delitos informáticos. A partir de allí, analizaremos las conductas ilícitas que lo afectan y la forma como el citado derecho, no es protegido adecuadamente debido al vacío existente en el ámbito penal, lo que no refleja los preceptos relativos a estos bienes jurídicos en la CPE.

"..., la identificación del bien jurídico tutelado penalmente, permite estimar si el delito informático en realidad protege algún nuevo interés social, que según la tratadista Gutiérrez Francés, es 'la información: (almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos) el bien jurídico que pone en peligro el delito informático". (Alessandri: 2010:45).

Además de poseer la información, en la actualidad es necesario poseer la capacidad de almacenarla, tratarla y transmitirla de forma eficaz. Por ello, en la información participan los elementos de almacenamiento, tratamiento y transmisión. En

este sentido y según esta escuela, el interés social pasible de protección penal es la información almacenada, tratada y transmitida a través de sistemas informáticos.

2.13.1. La información como bien jurídico intermedio

La sanción para evitar o sancionar la afectación de los derechos fundamentales de las personas, es un criterio que se ha venido desarrollando en el derecho penal a través de la historia. En este sentido, los atentados contra los bienes jurídicos necesarios para la existencia digna de las personas, no se limitan a las agresiones directas y personales sino que también pueden efectuarse a través de ataques indirectos e impersonales. (Por ejemplo el bien jurídico de la vida puede afectarse envenenando a una persona o también contaminando el agua potable de uso en una determinada población.) Es en este último caso en el que se aplica la noción de los bienes jurídicos intermedios, es decir aquellos: "intereses colectivos tutelados penalmente de forma conjunta con bienes de los particulares, siendo ambos de carácter homogéneo o estando situados en la misma línea de ataque" (Alessandri: 2010:48).

La caracterización de los bienes jurídicos intermedios comprende los siguientes elementos:

- Están vinculados con un bien jurídico netamente personal
- Tienen un carácter supra personal, (superan los intereses particulares);
- Corresponden a los intereses de la comunidad ya que poseen una mayor relación con los bienes individuales;
- Son equivalentes a los intereses individuales que puedan resultar vulnerados. (Por ejemplo, la relación entre no contaminación del medio ambiente y salud personal.).
- Tienen una relación instrumental entre bien colectivo y bien individual (el primer bien es un medio necesario para la puesta en peligro del segundo).
- La lesión de un bien jurídico intermedio constituye un riesgo potencial para un número no determinado de potenciales víctimas (Alessandri: 2010:49).

A partir de lo expuesto se puede concluir que el derecho a la información, constituye un bien jurídico intermedio, al comprender las características expuestas.

"El derecho a la información es un derecho colectivo en sus aspectos de confidencialidad, integridad y disponibilidad. Este derecho se plasma en un sentimiento de seguridad en la convivencia social por cuanto, en lo que respecta a la confidencialidad en la sociedad actual, la comunidad tiene derecho a la privacidad de los datos sobre su vida personal; comunicaciones, secretos industriales, etc., Así mismo, la comunidad tiene derecho a la autenticidad e integridad de la información ya que lo contrario implica un obstáculo para la normal convivencia. Por último, la comunidad también tiene derecho a la disponibilidad de la información sin obstáculos, para poder ejercer libremente sus derechos. (Alessandri: 2010:57)

"La sanción a las violaciones del derecho a la información, en lo relacionado a confidencialidad, integridad y disponibilidad, no son delitos de peligro abstracto ya que lesionan el bien jurídico intermedio afectando intereses individuales". (Alessandri: 2010: 51).

El considerar la información como bien jurídico intermedio, tal y como lo plantea la escuela estudiada, permite delegar y refrenda sancionar conductas que lesionan este derecho colectivo y ponen en peligro intereses individuales.

CAPITULO III
MARCO JURÍDICO

3.1. DETERMINACIÓN DE LA PENAL LEGAL

El objetivo del presente capitulo, es realizar el análisis de las convenciones internacionales, la normativa legal comparada y nacional existente sobre los delitos informáticos y de forma especial sobre el delito de suplantación de identidad, la doctrina en Derecho penal sobre los delitos informáticos y de forma especial sobre el delito de suplantación de identidad.

La determinación de la pena legal a nivel Legislativo, ocurre al crear una ley formal, donde establece una determinada pena a una conducta específica. Así el legislador señala la pena o medida de la pena en cada delito, de un modo general y abstracto. Para ello se toma en cuenta las especificaciones del tipo y las pautas de la Parte General de los Códigos Penales. Respecto a los elementos de la determinación de la pena. Tienen relevancia en nuestro sistema de justicia la gravedad del delito, que se refiere al grado de puesta en peligro del bien jurídico protegido, es decir, la entidad del daño producido al bien jurídico protegido y la forma de la ejecución del hecho. Este último consiste en la naturaleza de la acción y los medios empleados para llevarla a cabo. Asimismo se emplea el principio de analogía (Cusicanqui: 2011:18) Estos principios deben guiar la estructuración del anteproyecto de ley, sin embargo, debería considerarse la revisión de los dos artículos sobre delitos informáticos ya que parecería no haber la adecuada correspondencia al grado de puesta en peligro del bien jurídico protegido, sobretodo en el caso del segundo artículo.

3.1.1. La evolución del Derecho Penal y los delitos informáticos.

A nivel internacional el Derecho Penal ha evolucionado basándose en los principios de fragmentariedad, subsidiariedad y mínima intervención, según los cuales el *ius puniendi* debe ejercerse tan sólo ante las más graves vulneraciones de los intereses

sociales y siempre que no existan formas de control social menos gravosas que el control penal. En este sentido, el derecho penal en general por un lado ha restringido su ámbito de acción, al descriminalizar algunas conductas y en otros casos, como en el del ámbito cibernético, buscando reprimir nuevas conductas dañosas. Este proceso se origina como consecuencia de la evolución social, hecho que debe plasmarse en el ordenamiento penal ya que el cambio es un elemento propio de todo grupo social. El cambio en el ámbito de estudio de la presente investigación está estrechamente vinculado a la reciente evolución tecnológica que ha creado problemas para la protección de intereses sociales.

Las sociedades desarrolladas debido al impacto de la innovación tecnológica, han creado las primeras normas relativas a la cuestión. Así tenemos que en los 70 se promulgaron las primeras leyes referidas al ámbito de la intimidad; en la década de los 80 las leyes relacionadas con el resguardo de la propiedad intelectual de los programas (software) y en la década de los 90 las normas vinculadas al derecho a la información". ([52]).

Esta situación, se ha trasladado a sociedades como la nuestra implicando la necesidad de regularla. Según Gelhard existen cinco causas determinantes para que la informática se constituya en un fenómeno con importancia para el Derecho Penal.

Estas causas permiten establecer con claridad el potencial de peligrosidad para los bienes jurídicos protegidos no solo a escala internacional sino también nacional, ya que el desarrollo tecnológico también se ha introducido en nuestro país por la globalización.

3.1.2. El delito informático y su normativa internacional:

En la actualidad aún no se ha establecido un consenso en las posiciones jurídicas en torno al empleo ilícito de sistemas informáticos. Las normas son aisladas y sin carácter universal. Así por ejemplo el Art. 61 del acuerdo GATT de la Organización Mundial de Comercio (OMC) establece que para la falsificación dolosa de marcas de fábrica o de piratería lesiva del derecho de autor se establecerán los respectivos procedimientos y

[52] Gelhard: La evolución del Derecho Penal y los delitos informáticos. Edit. Mc Graw Hill. México 2011: pg. 108

sanciones penales. La Organización de Cooperación y Desarrollo Económico (OCDE) en 1983 realizó un estudio para aplicar y armonizar en el plano internacional las leyes penales, en torno a los programas de computación y en 1986 se publicó un informe sobre delitos de informática pero no hubo la armonización recomendada. En 1990 la Organización de las Naciones Unidas publico una topología de delitos Informáticos, sin embargo los países miembros poseen clasificaciones propias y divergentes. En 1992 La Asociación Internacional de Derecho Penal realizo recomendaciones respecto a promover la modificación de la definición de los delitos existentes y/o la creación de nuevos. Existen otros Convenios realizados por la Organización Mundial de la Propiedad Intelectual. En 1997 las II Jornadas Internacionales sobre el Delito Cibernético desarrollaron un marco legal y Deontológico de la Informática. En 2001 se efectuó el Convenio sobre la Ciberdelincuencia en Budapest con el fin de determinar un marco de referencia para las tecnologías y los delitos informáticos en la Unión Europea. (Sarzana: 2009:23-26).

A pesar de lo señalado, los mayores esfuerzos en materia de combate a los delitos cibernéticos se han dado a nivel interno de los estados, como veremos a continuación, debido a que el Derecho Penal es todavía fundamentalmente un asunto de carácter nacional. Respecto a la situación internacional cabe destacar que El Manual de las Naciones Unidas para la Prevención y Control de Delitos Informáticos identifica los siguientes problemas para la cooperación internacional en el ámbito de los delitos informáticos:

- Carácter trasnacional de muchos delitos cibernéticos, lo que exige una cooperación y acuerdos todavía inexistentes.
- Falta de tratados de extradición, de ayuda mutua y de mecanismos complementarios.
- Ausencia de acuerdos mundiales acerca de qué tipo de conductas deben constituir delitos informáticos.
- Carencias en especialización de los policías y funcionarios judiciales en el ámbito del delito informático.

- Ausencia de armonización entre las diferentes leyes procesales nacionales acerca de la investigación de los delitos informáticos. (Sarzana: 2009:109-114).

Como se ha podido observar, es indispensable continuar el proceso de modernización del derecho penal nacional para adecuarlo a los estándares internacionales.

3.2. SITUACIÓN DE LOS DELITOS INFORMÁTICOS EN BOLIVIA.

Los delitos informáticos en los últimos tiempos, han crecido exponencialmente en nuestro país y es así que tenemos que:

¨De 2002 a 2011, los juicios por delitos informáticos crecieron en un 890%, es decir de ocho a 79, (62 están referidos a manipulación informática y 17, a la alteración, acceso y uso indebido de datos informáticos). Aparte, en esa década, los juzgados de la Paz recibieron 228 causas referidas al primer delito y 15 del segundo. Asimismo, en el primer semestre meses de este año, ya se procesan 29 causas: 27 que incumben al artículo 363 bis y dos al artículo 363 ter del Código Penal¨ (Herbas :2012:8).

Siendo estos últimos los únicos dos delitos tipificados en nuestra legislación, mientras que la ONU establece más de 10, como se dijo anteriormente. En otras palabras, esta estadística solo se refiere a una parte de la delincuencia informática que se realiza en nuestro país. Las estadísticas proporcionadas por la FELCC y el Consejo de la Magistratura de La Paz al diario La Razón establecen:

574 denuncias referidas a manipulación informática en ocho departamentos, excluyendo a Oruro. Un 2% más que las 562 que ocurrieron en 2010. En 2011, el mayor número de casos se registró en Santa Cruz, con un total de 486; seguido por La Paz, donde se presentaron 69. Lo llamativo es que ambas regiones concentran más del 95% de éstos, o sea, 555 de los 574. Posteriormente se ubican Cochabamba, con ocho; Chuquisaca, con cuatro; Tarija, con tres; Beni, con dos, y Pando y Potosí con uno cada uno. Aparte, desde enero hasta marzo de este año ya se suman 47 denuncias en las

dependencias policiales. Sobre el delito de alteración, acceso y uso indebido de datos informáticos la Policía no cuenta con estadísticas a nivel Nacional (Herbas: 2012:8).

Según datos proporcionados por la FELCC, el delito informático y hechos relacionados con este delito actualmente no tipificados en nuestra legislación a veces no llegan a ser investigados por las autoridades porque no son denunciados por las víctimas, por desconfianza en el sistema judicial o porque las sanciones son casi simbólicas o por el desconocimiento de los damnificados de que hay peritos policiales y del Ministerio Público que investigan estos casos. Asimismo entre los problemas a superar en este ámbito cabe mencionar un obstáculo de naturaleza jurídica ya que más allá de la necesidad de actualizar el Código Penal en materia de delitos informáticos, el nuevo Código Procesal Penal, debe establecer el principio de "libertad probatoria" de forma que los testigos puedan presentar soportes informáticos como pruebas, con características de autenticidad, precisión y suficiencia para su validez jurídica. En relación a la Jurisprudencia cuando se imputa a una persona por un delito informático, la imputación incluye además otros delitos con más o menos años de cárcel, por ejemplo abuso de confianza, hurto, uso de instrumento falsificado, estafa agravada, etc. Esto se da porque si bien se pueden manipular los datos de entrada, el proceso o la salida de datos, estos datos en algún momento se reflejan en un papel firmado/rubricado o para causar el daño patrimonial establecido en el 363 bis, alguien deberá recibir el dinero físicamente. Los delitos informáticos en muchos casos no se castigan por defectos procesales, al igual que otro tipo de delitos, en este punto debemos resaltar la falta de capacitación del Personal de la fuerza de la Ley en el secuestro de evidencia digital y la preservación de la cadena de custodia de la misma. Es en este marco situacional que por ejemplo la Agencia Boliviana Para el Desarrollo de la Información ha planteado un proyecto de ley para cambiar los dos tipos penales mencionados en nuestro código penal e incrementar la sanción penal así como implementar nuevas figuras delictivas como el sabotaje informático, la falsificación y suplantación de identidad electrónica, delitos que ya figuran en legislaciones de otros países. (Herbas: 2012:8-9).

3.2.1. Marco Legal de los delitos Informáticos en Bolivia:

En nuestro país los delitos informáticos entendidos como los actos que provocan la comisión de agravios, daños o perjuicios en contra de las personas, grupos, entidades o instituciones, y que son ejecutados por medio de computadoras, son regulados como delitos comunes, los mismos que, de forma genérica y parcial se encuentran incorporados en el Código Penal ya que carecen de una ley específica. Desgraciadamente el código penal solo tipifica dos delitos, manipulación informática y acceso indebido, de los más de diez delitos establecidos por la ONU. Los dos Artículos dentro del texto ordenado según el Código Penal ley No 1768 de1997 a la letra establecen:

CAPITULO XI

DELITOS INFORMATICOS

> ***Artículo 363.- BIS (MANIPULACION INFORMATICA****). 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.*
>
> *Articulo 363.- TER (ALTERACION, ACCESO Y USO INDEBIDO DE DATOS INFORMATICOS). 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.".(CODIGO PENAL: 2010. 34).*

Cabe resaltar que el segundo artículo citado no establece pena de cárcel, lo cual puede no es proporcional al bien jurídico afectado. Todos los actos contrarios a la ley en que se empleen herramientas electrónicas, son agrupados solo en estos dos preceptos del Código Penal, aunque existen delitos informáticos que también pueden ser castigados con lo estipulado en otras figuras penales semejantes; por ejemplo, en el caso de una estafa realizada con páginas de internet o correos electrónicos, se aplicaría el artículo 335 de estafa. En relación a las estafas informáticas los ataques de manera informática a cuentas bancarias se consideran delitos penales comunes. Así como en los casos

comentados, estos dos delitos (manipulación y acceso indebido) se pueden vincular con otros, como son el robo, hurto, uso de instrumento falsificado, abuso de confianza y otros. En el marco de lo expuesto, la criminalidad informática puede afectar a bienes jurídicos tradicionalmente protegidos, como en el caso de delitos en los que se emplea una computadora para redactar una carta difamando a personas físicas o jurídicas, o atentar contra la integridad personal, etc. En otros casos las conductas lesionan bienes no protegidos tradicionalmente por la legislación penal, tal el caso de los bienes Informáticos, consistentes en datos, información computarizada, archivos y programas, como el fraude electrónico y el sabotaje informático. Situación complicada que no ayuda a la claridad en materia penal ni a las labores del juez. En la actual CPE, el Artículo referentes al tema de Delitos Informáticos en lo que hace al habeas data, establece:

> ***SECCIÓN III***
> ***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 y familiar, a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.(Constitución Política del Estado:2011: 49).*

Respecto al derecho a la imagen podría conceptualizarse, como la facultad que tiene su titular de difundir o publicar su propia imagen; y derivado de ello, a que terceros no la reproduzcan o publiquen, sin su consentimiento, cuando entiende que daña su honor, reputación intimidad, o decoro. La Constitución no consagra de manera expresa el derecho a la imagen aunque si lo hace el Código civil, Articulo 16 estableciendo que:

> *"Cuando se comercia, publica, exhibe o expone una imagen de una persona lesionando su reputación o decoro, la parte interesada y, en su defecto, su cónyuge, descendientes o ascendientes pueden pedir, salvo los casos justificados por ley, que el juez haga cesar el hecho lesivo".* ([53]).

[53] GACETA OFICIAL DE BOLIVIA; Código Civil Boliviano

En todo caso, la no consagración expresa del derecho a la imagen, no impide que, al tratarse de un derecho inherente a la persona humana, pueda encontrar protección a través de los recursos previstos en la Constitución, ya que el derecho a la imagen es un derecho humano que involucra la facultad de proteger la imagen propia. Sin embargo, también cabe referir su protección en el orden internacional a través de diversos instrumentos sobre derechos humanos. (Willman: 2011:34).

Otros delitos cibernéticos, están establecidos en la Ley de Telecomunicaciones. Sin embargo las sanciones están sujetas a reglamentación, aun inexistente a la fecha. Asimismo y lamentablemente esta Ley tiene mucha diferencia con relación al proyecto que se presentó inicialmente, particularmente en los referente a los Delitos Informáticos que ya no contempla las inclusiones al código penal en falsedad material, documental, ideológica, etc. y otros aspectos que también tiene una relación directa o indirecta con la suplantación de identidad electrónica y que se encontraban en el proyecto. Sin embargo, como se indicó anteriormente, las sanciones para estos delitos están mencionadas en el artículo 92, sin especificar los delitos cibernéticos:

> *"Constituyen infracciones dentro el marco regulatorio las transgresiones a las disposiciones contenidas en la presente Ley y sus reglamentos, contratos y otras normas aplicables al sector de telecomunicaciones y tecnologías de información y comunicación". (Ley de Telecomunicaciones: 2011: 14).*

Así también tenemos las siguientes disposiciones relativas a nuestra temática:

TÍTULO V

INFRACCIONES Y SANCIONES

Artículo 92. (INFRACCIONES). Constituyen infracciones dentro el marco regulatorio las transgresiones a las disposiciones contenidas en la presente Ley y sus reglamentos, contratos y otras normas aplicables al sector de telecomunicaciones y tecnologías de información y comunicación.

Artículo 93. (CRITERIOS). Las sanciones serán determinadas teniendo en cuenta los siguientes criterios:

1. Naturaleza y gravedad del hecho.
2. Extensión y magnitud del peligro o daño causado.
3. Dolo o culpa en la comisión de la infracción.
4. Existencia de agravantes y atenuantes en la comisión de la infracción.

Artículo 94. (SANCIONES).

I. Sin perjuicio de la acción penal que corresponda, la Autoridad de Regulación y Fiscalización de Telecomunicaciones y Transportes, aplicará a los infractores las sanciones de apercibimiento, secuestro o embargo de equipos y material, multas e inhabilitación temporal para ejercer las actividades en telecomunicaciones y tecnologías de información y comunicación.

Artículo 99. (CLASIFICACIÓN).

I. Las infracciones, teniendo en cuenta el objeto de las mismas, se clasifican en infracciones:
    1. Por prestación ilegal del servicio, ejercicio ilegal de actividades de telecomunicaciones y tecnologías de información y comunicación y por utilización indebida del espectro radioeléctrico.
    2. Contra el sistema de telecomunicaciones.
    3. Contra los derechos de las usuarias y los usuarios.
    4. Contra los derechos de los operadores y proveedores.
    5. Contra las atribuciones de la autoridad fiscalizadora.
    6. Otras infracciones.

II. Las sanciones se aplicarán teniendo en cuenta la gravedad de las infracciones.

III. La tipificación o individualización de las infracciones serán establecidas en reglamento

Artículo 108. (INFRACCIONES Y SANCIONES).

Constituyen infracciones administrativas las transgresiones a las disposiciones contenidas en la presente Ley, sus reglamentos, contratos y otras normas aplicables al sector postal.

VII. La tipificación o individualización serán establecidas en reglamento. (Ley de Telecomunicaciones: 2011: 15-18).

La carencia de un reglamento para estas normas causa serios problemas a nuestro sistema judicial, ya que esta Ley, al ser promulgada entra en vigencia de manera inmediata, sin embargo los delitos de este tipo, no pueden ser sancionados en los hechos. El principio básico del derecho que establece que lo que no está prohibido está permitido; no permite sancionar este tipo de conducta porque no está tipificada como delito. Sin embargo, las nuevas modalidades delictivas mencionadas, que por diferentes razones es difícil reprimir penalmente, son criminógenas. Es por ello que el Código Penal también debe ser modificado para que se tipifiquen y sancionen estas nuevas conductas, que por su especial naturaleza no pueden encuadrarse mecánicamente en las figuras convencionales sino que es necesario que se creen nuevos tipos. Esta necesidad es normal ya que, como es sabido, cada cierto tiempo el Derecho Penal sufre una desactualización, debido a los cambios y desarrollos históricos y por ello requiere reformas. Aunque los delitos informáticos están tipificados en el Código Penal (artículo 363 bis y 363 ter), éstos se limitan a la manipulación, alteración, acceso y uso indebido de datos cibernéticos. Sin embargo la suplantación de identidad vinculada con pornografía infantil, difamación de imagen, extorsión y amenazas realizadas a través de sistemas informáticos no figuran.

3.3. LA SUPLANTACIÓN DE IDENTIDAD ELECTRÓNICA Y LOS DELITOS INFORMÁTICOS EN SU RELACIÓN CON TIPOS PENALES TRADICIONALES DEL DERECHO PENAL BOLIVIANO.

El vacío legal en relación a la suplantación de identidad electrónica, no implica que puedan existir conductas que reúnen elementos constitutivos de algunos tipos penales tradicionales, Por ejemplo: El "Artículo 363º. Ter. (ALTERACIÓN, ACCESO Y USO INDEBIDO DE DATOS INFORMÁTICOS) en ciertas circunstancias se adecúa mejor cuando existen casos de Apropiación de Identidad Digital sin embargo, también podemos considerar, cuando la Suplantación de Identidad Digital se realiza a través de redes

sociales como facebook, correos electrónicos, etc., se tendría una estrecha relación con el : “Artículo 282º. (DIFAMACIÓN) del Código Penal.. Lo mismo puede ocurrir en relación al “Artículo 287º. (INJURIA). Asimismo, la suplantación de identidad puede tener relación con el “Artículo 293º. (AMENAZAS). Considerando que en nuestro país los mensajes electrónicos y de celular, son medios comunes para amedrentar a las personas, amenazarlos y/o coaccionarlos la suplantación de identidad puede tener relación con el Artículo 294º. (COACCIÓN). La suplantación de identidad a nivel empresarial, se emplea para el desvío de clientela por lo que podría tener relación con el “Artículo 237º. (DESVÍO DE CLIENTELA). En el caso de suplantación de identidad vinculada con pedofilia, secuestro y otros delitos afines donde se contacta a la víctima mediante alguna red social o e-mail, engañando sobre la identidad, existe relación con el “Artículo 246º. (SUBSTRACCIÓN DE UN MENOR O INCAPAZ). Asimismo en caso de publicaciones de contenido sexual de pedofilia logrados a través de la suplantación de identidad o secuestro se tiene relación con el “Artículo 324º. (PUBLICACIONES Y ESPECTACULOS OBSCENOS).

Respecto a la TRATA Y TRAFICO DE PERSONAS Y OTROS DELITOS RELACIONADOS tenemos relación con los siguientes artículos: “Artículo 281 bis (Trata de Seres Humanos), Artículo 281 ter (Tráfico de Migrantes), Artículo 132 bis (Organización Criminal). Asimismo la suplantación de identidad puede guardar relación con el proxenetismo: Artículo 321 (Proxenetismo). Asimismo la suplantación puede tener relación con la extorsión y la estafa:

Respecto al derecho a la imagen el Código Civil en su artículo 16 (Derecho a la imagen) señala que si se comercia, publica, exhibe o expone la imagen de una persona lesionando su reputación o decoro, la parte interesada, y en su defecto su cónyuge o descendientes, pueden pedir que el juez haga cesar el hecho; en el artículo 18, se indica que nadie puede perturbar ni divulgar la vida íntima de una persona, mientras que el artículo 23 establece que los derechos de personalidad son inviolables.

En el marco de lo anotado la suplantación de identidad tiene una relación estrecha con la falsedad ideológica y material, específicamente con: CAPITULO III FALSIFICACION DE DOCUMENTOS EN GENERAL Artículo 198°.- (FALSEDAD MATERIAL), el Artículo 199°.- (FALSEDAD IDEOLOGICA). El Artículo 200°.- (FALSIFICACION DE DOCUMENTO PRIVADO). Y el Artículo 203°.- (USO DE INSTRUMENTO FALSIFICADO). ([54]).

La situación descrita muestra el alto grado de relacionamiento de la suplantación de identidad con otros ilícitos de lo cual se puede inferir su elevada peligrosidad.([55])

3.4. SUPLANTACIÓN DE IDENTIDAD

La identidad es un concepto amplio con dimensiones culturales, antropológicas, psicológicas, etc., y que tiene relación con un conjunto de datos que caracterizan a un determinado sujeto y que en Derecho es relevante en términos de identificación personal siendo definida de la siguiente manera:

"…el hecho comprobado de ser una persona, constituyendo la determinación de la personalidad a los efectos de las relaciones jurídicas…"(Cabanellas:2004:195).

En el marco de lo expuesto, son los factores que permiten la individualización e identificación de una persona (datos biométricos como firma, huellas dactilares, fondo de los ojos, etc.) los que son objeto de manipulación o falsificación en los casos de suplantación de identidad.

La definición jurídica de suplantación de identidad varía ampliamente de acuerdo al marco jurídico respectivo de cada país. Sin embargo, el término es comúnmente utilizado para describir que la información personal de un individuo (información, financiera, médica, etc.) ha sido obtenida y utilizada sin su consentimiento y con el propósito de

[54] CODIGO PENAL: 2010. 10-67

[55] Michel CLAUDIA ARAUJO "Robo de identidad digital: un tema pendiente en la ley boliviana"; http://www.nobosti.com/spip.php?article1322

cometer actividades ilícitas. La suplantación de identidad normalmente involucra la adopción de la identidad de una persona como pudiera ser su nombre, fecha de nacimiento, dirección, números de licencia y de seguridad social, etc. En este sentido general, la suplantación de identidad, falsificación de documentos o uso de instrumento falsificado, son delitos tipificados en el Código Penal boliviano. Asimismo El Código Civil en su artículo 9 establece:

> *Cuando se comercia, publica, exhibe o expone la imagen de una persona lesionando su reputación o decoro, la parte interesada Y, en su defecto, su conyugue, descendientes o ascendientes pueden pedir, salvo los casos justificados por ley, que el juez haga cesar el hecho lesivo" (Código Civil:2004:24.).*

En este mismo sentido, La CPE. Estatuye el derecho a la identidad en su artículo 59 IV:

> *"Toda niña, niño o adolescente tiene derecho a la identidad y la filiación respecto a sus progenitores" (Constitución Política del estado:2009:20).*

3.4.1. Suplantación de identidad electrónica

Se entiende como suplantación de personalidad o identidad electrónica cuando alguien finge ser una persona que no es, es decir el hecho de una persona valerse de una identidad ajena a la suya, a través de medios electrónicos, informáticos, telemáticos o de telecomunicaciones. La Suplantación de Identidad Electrónica ocurre cuando una parte adquiere, transfiere, posee o usa información personal de una persona física o jurídica sin la autorización respectiva, con la intención de cometer fraude u otros delitos relacionados, sea por Internet u otro medio electrónico. Las formas de suplantar la identidad son variadas y con el paso de los años han ido evolucionando, tanto en técnica como tecnológicamente. El robo o la suplantación de identidad es el delito informático de más rápido crecimiento en el mundo y que se comete con más regularidad en los países donde el uso del Internet es el medio común para compras, pagar impuestos realizar transferencias etc. (Gelhard: 2011:94).

En Estados Unidos, cada cuatro segundos es robada una identidad y se afecta alrededor de 10 millones de personas por año, creando un perjuicio aproximado de 50 billones de dólares. la restauración de la identidad de una persona cuesta 8 mil dólares y se pierden 600 horas aproximadamente para realizar los trámites correspondientes. (Gelhard: 2011:94).

En nuestro país por la debilidad institucional, carencia de tipificación y falta de denuncias, no existen datos estadísticos sobre usurpación de identidad, aunque por su vinculación con otros delitos se sabe que, como en el resto del mundo, es el delito informático de mayor crecimiento en los últimos anos.

Si bien la usurpación de identidad no está tipificada en nuestro cuerpo normativo, se debe destacar que por medio de la misma, en calidad de acto preparatorio, se cometen gran cantidad de delitos. Por ejemplo los pedófilos utilizan identidades falsas para engañar a sus víctimas, un chantajista puede ocultar sus propósitos o amenazar a su víctima desde el anonimato, etc. Asimismo, los delitos informáticos están contemplados en la legislación, pero no se hace referencia a los daños que puede hacerse contra una persona a través de esos mismos medios. Las dos figuras que reconoce la legislación penal están fuera de contexto en relación con la protección de la imagen y la dignidad de la persona como tal, incluso una persona jurídica, ya que se pueden afectar instituciones.

3.4.2. Tipos de Suplantación electrónica:

De forma general los tipos de suplantación electrónica son:

Phising:

Es un fraude por suplantación de identidad. El origen de la palabra phishing proviene del inglés “password harvesting fishing” (cosecha y pesca de contraseñas) Las personas que realizan el fraude buscan la obtención de información personal de las víctimas como números de tarjetas de crédito, cuentas bancarias, contraseñas, etc. Para lograr obtener esta información existen formas distintas como envío de mensajes de correo electrónico fraudulentos, mensajería instantánea o falsos sitios web etc.

Scam:

Este tipo de fraude consiste en que empresas ficticias realizan la captación de personas mediante diversas vías como (correo electrónico, foros, anuncios en donde ofrecen puestos de trabajo, etc.,) y cuyas condiciones son disponer de una computadora y ser titular de una cuenta bancaria para el blanqueo de dinero obtenido a través del phishing, acto que se realiza sin conocimiento de la víctima.

Hoax:

Se trata de mensajes que se distribuyen en cadena. Se caracterizan por atemorizar al destinatario si no continúa con la cadena de mensajes. Los objetivos de este tipo de fraude son conseguir direcciones de correo electrónico, colapsar servidores, etc.

AFF:

Se trata de un engaño para que la víctima pague una cantidad de dinero por adelantado para recibir un determinado regalo o premio. El fraude por adelanto de pago (AFF Advance Fee Fraud) es conocido también como fraude de la lotería y constituye una de las formas más peligrosas. Para dar mayor credibilidad a sus mensajes de correo electrónico los delincuentes simulan páginas de compañías de prestigio.

Spoofing:

El spoofing también es una suplantación de identidad, pero en la cual no se requiere por lo general de un engaño previo a la víctima o a la entidad.

IP:

Consiste en la modificación de paquetes informáticos de forma que la dirección de origen (IP) no es real, sino la de quien se va a suplantar (modificación del remitente).

ARP:

Esta suplantación trabaja en una red Ethernet conmutada de forma que todos los paquetes que la máquina víctima son recibidos por la máquina atacante. El atacante determina si espía a la víctima o simplemente le incomunica asociándola una dirección inexistente.

DNS:

También llamado pharming, se trata del cambio de la relación de un nombre de un dominio por una IP falsa.

Web:

En esta modalidad se suplanta la dirección real por una página falsa que recolectará información de la víctima. Esta página falsa actuará a modo de proxy (intermediario), de forma que recolectará toda la información de la comunicación de la víctima.

Mail:

En este caso se envían correos con un remitente falso. Las intenciones pueden ser variadas, como complemento para phising, o para distribuir rumores, etc. (Sarzana: 2009:27-29).

Asimismo la información obtenida mediante algunos de los tipos de suplantación electrónica mencionados puede servir para solicitar en nombre de una tercera persona créditos, así como realizar operaciones de cobro de ahorros o pólizas o clonación de tarjetas de débito y crédito para adquirir bienes ilícitamente, sin que la persona afectada tenga conocimiento de ello. Asimismo, puede dar lugar a la falsificación de documentos personales (cédula de identidad, firma del titular, fotografía e impresión digital) para diferentes propósitos delictivos.

En nuestro país los recientes casos de clonación de tarjetas de débito y crédito afectados por la suplantación de identidad mediante el pishing en los primeros cuatro meses de 2011, han ocasionado pérdidas de alrededor de 1,5 millones de bolivianos para

clientes de diferentes bancos en las ciudades del eje troncal (Heredia: 2012:8). Otra modalidad frecuentemente utilizada es la suplantación de identidad mediante la falsificación de documentos personales (cédula de identidad) para obtener créditos. Finalmente, la falsificación de páginas web de entidades financieras para solicitar actualización de datos personales vía Internet, es otra modalidad.

El delito informático financiero, tipificado en el Código Penal como manipulación informática y/o alternación, acceso y uso de datos, establece sanciones que no guardan relación con los montos defraudados. Si el robo es de cinco bolivianos o de un millón, la pena máxima, para ambos casos, no es mayor a cinco años, además que por la presentación de recursos judiciales, los acusados pueden pasar alrededor de un año en la cárcel. No todos los fines de la suplantación de identidad son de carácter económico. También responden a motivaciones de venganza personal, descredito político, etc. (Estas motivaciones no económicas son comunes respecto a personajes públicos como políticos, artistas, o periodistas). Por ejemplo la suplantación de René Martínez en Facebook, para tomar contacto con los simpatizantes del Movimiento Al Socialismo, y emitir supuestos comentarios de e insultos que desacreditaban al supuesto titular de la página.

El asambleísta fue víctima de la suplantación de su identidad durante meses en 2010, lo que violaba su identidad digital en internet. En abril de 2010, la gerente general del Servicio de Desarrollo de las Empresas Públicas Productivas, Patricia Ballivián, presentó a la Fuerza Especial de Lucha Contra el Crimen la denuncia por el delito de discriminación contra los creadores de una publicación en la red social Facebook, en la que se denigra a sus hijas y a ella. (Heredia: 2012:8) En muchos casos el delincuente descifra mediante programas especiales la contraseña de correo electrónico o del perfil de las redes sociales de su víctima. En otros casos, el damnificado no tiene cuenta en una determinada red social como Facebook, lo que abre las puertas a que cualquiera pueda abrir una cuenta con su identidad. En este sentido al querer iniciar acciones legales en su defensa, las victimas se encuentran con obstáculos serios que van desde los procedimentales hasta de cómo demostrar quién es el autor del hecho delictivo. Por

ejemplo se puede llegar a establecer desde qué equipo o dirección IP, se ha cometido la suplantación, pero no se puede identificar con absoluta certeza quien es el autor del mismo, a no ser que se utilicen otros medios probatorios del Código de Procedimiento Penal. Es así que en nuestro medio cada vez más se van acrecentando los casos de suplantaciones de Identidad en correos electrónicos, redes sociales, etc.; por lo que empresas y personas, se ven frente a la no regulación específica sobre la cuestión.

3.5. DELITOS INFORMÁTICOS Y SU INTERNACIONALIZACIÓN

3.5.1. Organismos internacionales

El objetivo de este capítulo es presentar todos aquellos elementos que han sido considerados tanto por organismos gubernamentales internacionales así como por diferentes Estados, para enfrentar la problemática de los delitos informáticos a fin de que contribuyan al desarrollo de la presente investigación.

En este orden, debe mencionarse que durante los últimos años se ha ido perfilando en el ámbito internacional un cierto consenso en las valoraciones político-jurídicas de los problemas derivados del mal uso que se hace de las computadoras, lo cual ha dado lugar a que, en algunos casos, se modifiquen los derechos penales nacionales.

En un primer término, se debe considerar que en 1983, la Organización de Cooperación y Desarrollo Económico (OCDE)[56] inició un estudio de la posibilidad de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.

De esta forma, la OCDE. en 1986 publicó un informe titulado Delitos de Informática: análisis de la normativa jurídica, en donde se reseñaban las normas

[56] Ver: OECD: Organización para la Cooperación Económica y el Desarrollo. *Computer related criminalliy: analisys of legal policy in the OECD area*, ICCP, 84:22, 1984. Disponible en: http://www.informatica-uridica.com/trabajos/Criminalidad_informatica_en_Bolivia. Recuperado el: 16-05-1996.

legislativas vigentes y las propuestas de reformas en diversos Estados Miembros y se recomendaba una lista mínima de ejemplos de uso indebido que los países podrían prohibir y sancionar en leyes penales (Lista Mínima); como por ejemplo: el fraude y la falsificación informáticos, la 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.

La mayoría de los miembros de la Comisión Política de Información, Computadores y Comunicaciones recomendó también que se instituyesen protecciones penales contra otros usos indebidos (Lista optativa o facultativa), espionaje informático, utilización no autorizada de una computadora, utilización no autorizada de un programa protegido, incluido el robo de secretos comerciales y el acceso o empleo no autorizado de sistemas de computadoras.

Con objeto de que se finalizara la preparación del informe de la OCDE, el Consejo de Europa inició su propio estudio sobre el tema a fin de elaborar directrices que ayudasen a los sectores legislativos a determinar qué tipo de conducta debía prohibirse en la legislación penal y la forma en que debía conseguirse ese objetivo, teniendo debidamente en cuenta el conflicto de intereses entre las libertades civiles y la necesidad de protección.

La lista mínima preparada por la OCDE. se amplió considerablemente, añadiéndose a ella otros tipos de abuso que se estimaba merecían la aplicación de la legislación penal. El Comité Especial de Expertos sobre Delitos relacionados con el empleo de computadoras, del Comité Europeo para los Problemas de la Delincuencia, examinó esas cuestiones y se ocupó también de otras, como la protección de la esfera personal, las víctimas, las posibilidades de prevención, asuntos de procedimiento como la investigación y confiscación internacional de bancos de datos y la cooperación internacional en la investigación y represión del delito informático.

Una vez desarrollado todo este proceso de elaboración de las normas a nivel continental, el Consejo de Europa aprobó la recomendación R (89) sobre delitos informáticos, en la que "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 para los legisladores nacionales". Esta recomendación fue adoptada por el Comité de Ministros del Consejo de Europa el 13 de septiembre de 1989. Las directrices para los legisladores nacionales incluyen una lista mínima, que refleja el consenso general del Comité, acerca de determinados casos de uso indebido de computadoras y que deben incluirse en el derecho penal, así como una lista facultativa que describe los actos que ya han sido tipificados como delitos en algunos Estado pero respecto de los cuales no se ha llegado todavía a un consenso internacional en favor de su tipificación.

Adicionalmente, se debe mencionar que 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 erigir, el mismo año, un marco de seguridad para los sistemas informáticos.

Por otra parte, a nivel de organizaciones intergubernamentales de carácter universal, debe destacarse que en el seno de la Organización de las Naciones Unidas (ONU), en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal, celebrado en 1990 en la Habana Cuba, se indicó que la delincuencia relacionada con la informática era consecuencia del mayor empleo del proceso de datos en las economías y burocracias de los distintos países y que por ello se había difundido la comisión de actos delictivos.

Además, la injerencia transnacional en los sistemas de proceso de datos de otros países, había traído la atención de todo el mundo. Por tal motivo, si bien el problema principal, hasta ese entonces, era la reproducción y la difusión no autorizada de programas informáticos y el uso indebido de los cajeros automáticos, no se habían

difundido otras formas de delitos informáticos, por lo que era necesario adoptar medidas preventivas para evitar su aumento.

En general, se supuso que habría un gran número de casos de delitos informáticos no registrados. Por todo ello, en vista de que los delitos informáticos eran un fenómeno nuevo, y debido a la ausencia de medidas que pudieran contrarrestarlos, se consideró que el uso deshonesto de las computadoras podría tener consecuencias desastrosas. A este respecto, 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.

Partiendo del estudio comparativo de las medidas que se han adoptado a nivel internacional para atender esta problemática, deben señalarse los problemas que enfrenta la cooperación internacional en la esfera del delito informático y el derecho penal, a saber: la falta de consenso sobre lo que son los delitos informáticos, la falta de definición jurídica de la conducta delictiva, la falta de conocimientos técnicos por parte de quienes hacen cumplir la ley, las dificultades de carácter procesal y la falta de armonización para investigaciones nacionales de delitos informáticos. Adicionalmente, se debe mencionar la ausencia de la equiparación de estos delitos en los tratados internacionales de extradición. Presente esa situación, se considera que es indispensable resaltar 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. 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.

En otro orden de ideas, debe mencionarse que la Asociación Internacional de Derecho Penal durante un coloquio celebrado en Wurzburgo 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 deberá tenerse en cuenta hasta qué punto el derecho penal se extiende a esferas afines con un criterio importante para ello como es el de limitar la responsabilidad penal con objeto de que éstos queden circunscritos primordialmente a los actos deliberados.

Asimismo, considerando el valor de los bienes intangibles de la informática y las posibilidades delictivas que pueden entrañar el adelanto tecnológico, se recomendó que los Estados consideraran de conformidad con sus tradiciones jurídicas y su cultura y con referencia a la aplicabilidad de su legislación vigente, la tipificación como delito punible de la conducta descrita en la "lista facultativa", especialmente la alteración de datos de computadora y el espionaje informático; así como que por lo que se refiere al delito de acceso no autorizado precisar más al respecto en virtud de los adelantos de la tecnología de la información y de la evolución del concepto de delincuencia.

Igualmente, se manifiesta que el tráfico con contraseñas informáticas obtenidas por medios inapropiados, la distribución de virus o de programas similares deben ser considerados también como susceptibles de penalización.

3.6. LEGISLACIÓN COMPARADA

Estas proceden en buena medida, de la prohibición jurídico-penal de analogía y en ocasiones, son insuperables por la vía jurisprudencial. De ello surge la necesidad de adoptar medidas legislativas. En los Estados industriales de Occidente existe un amplio

consenso sobre estas valoraciones, que se refleja en las reformas legales de los últimos diez años.

Pocos son los países que disponen de una legislación con referencia a la problemática abordada, sin embargo con objeto de que se tomen en cuenta las medidas adoptadas por ciertos países, a continuación se presenta los siguientes casos particulares:

3.6.1. La Legislación Chilena

En junio de 1998 se creó la "Comisión Nacional para las Nuevas Tecnologías de Información y Comunicación", en calidad de órgano asesor del Presidente de la República y bajo la dirección del Ministro de Economía, Fomento y Reconstrucción, cuya misión principal fue elaborar una visión prospectiva sobre las tendencias e impactos del desarrollo de las tecnologías de información y comunicaciones en nuestro país y elaborar una propuesta con lineamientos estratégicos y acciones concretas para potenciar la difusión de las nuevas tecnologías y redes a lo largo del país.

Para cumplir su labor esta entidad elaboró un informe, con un conjunto de recomendaciones e iniciativas, fruto del trabajo de más de cien personas.

El documento plantea, entre otras medidas, la necesidad de "iniciar el desarrollo de un marco jurídico que valide el uso del documento y la firma digitales, tanto para el Estado como para el desarrollo del comercio electrónico", recomendando como acción emblemática "estudiar a corto plazo la posibilidad de promulgar un decreto supremo para el sector público que legalice el uso del documento electrónico y la firma digital".[57]

3.6.2. La Legislación Argentina

El hecho tecnológico que se manifiesta con el avance de la informática y los medios informáticos en constante evolución, vienen a modificar las relaciones entre los sujetos debido a la irrupción de nuevas modalidades y distintos procedimientos, más veloces y

[57] Regulación Chilena de junio de 1998 por la que se creó la "Comisión Nacional para las Nuevas Tecnologías de Información y Comunicación".

precisos que nos han conducido a no identificar necesariamente los títulos circulatorios o el contrato con el papel que lo contiene en vías de reemplazo por el documento electrónico. En este sentido, el documento electrónico es considerado como cosa. La pregunta que cabe formularse es si el documento electrónico puede ser considerado una cosa.

Digiorgio advierte que se podría sostener que el documento electrónico constituye un objeto material de tener un valor, quedando encuadrado en la definición del Art. 2311 del Código Civil y además que, en algunos casos y bajo ciertas circunstancias, se puede obtener uno nuevo con iguales características, por lo que parecería sencillo entonces el autor afirma que la mera traslación del soporte papel al soporte electrónico o magnético no desnaturaliza su calidad de documento como cosa, atento a que nuestro Código Civil únicamente hace mención al papel en su Art. 1019.

El documento debe examinarse a partir de determinados sustratos como el soporte, la forma y la prueba. En cuanto al soporte, razones de practicidad (o lo que se denomina una cultura de papel) ha llevado a utilizar el papel como elemento preponderante pero no exclusivo.

Según opina Digiorgio, el documento electrónico puede incluirse en una categoría que había de denominarse bienes dinámicos, o más propiamente cosas dinámicas, por estar relacionadas o pertenecer a una fuerza que produce movimiento (alguno de estos objetos materiales constituyen cosas inasibles, toda vez que no pueden ser tocadas o sostenidas por las manos, criterio este que proviene de la concepción romanista).

Con lo cual este autor se inclina a considerar como cosa al documento electrónico si bien advierte que en algunas circunstancias constituyen objetos materiales intangibles, los que no se pueden percibir concretamente, esto es, no pueden percibirse de modo directo, pero que mediante la utilización de determinados procedimientos que funcionan con sus pertinentes equipos y aparatos, se pueden determinar, medir, valorar y utilizar, porque estos objetos tienen manifestaciones que llegan a nuestros sentidos y a nuestra

inteligencia, ya que podemos entenderlos, ordenarlos o bien dirigirlos racionalmente, por el cual quedan encuadrados en el concepto de cosa del Art. 2311 del Código Civil.[58]

3.6.3. La legislación de Perú

El ordenamiento jurídico peruano tipifica los siguientes delitos, los cuales se encuentran dentro del concepto de delitos informáticos que se ha dado en la primera parte de este trabajo. Estos son:

- Delitos informáticos
- Delito de violación a la intimidad (Art. 154 del Código Penal),
- Delito de hurto calificado por transferencia electrónica de fondos (Art. 186 Segundo párrafo numeral 3 del Código Penal, modificado por Ley 16.319)
- Delitos contra los derechos de autor (Art. 216 Código Penal),
- Delito de falsificación de documentos informáticos (Decreto Legislativo 681, Art. 19 – Art. 427 del Código Penal),
- Delito de fraude en la administración de personas jurídicas en la modalidad de uso de bienes informáticos (Art. 198 inc. 8 del Código Penal)
- Delito de daños aplicable al hardware (Art. 205 del Código Penal). [59]

3.6.4. Legislación de Austria

Se tiene la *Ley de reforma del Código Penal de 22 de diciembre de 1987*. Esta ley contempla los siguientes delitos[60]:

- Destrucción de datos (126). En este artículo se regulan no sólo los datos personales sino también los no personales y los programas.
- Estafa informática (148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el

[58] Nota: Se evidencia que en la República de Argentina, los delitos informáticos cuentan con una regulación parcial enfocada más en el campo del Derecho Civil.
[59] El Código Penal del Perú.
[60] Ley de reforma del Código Pena de Austria de 22 de diciembre de 1987.

resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

3.6.5. Legislación de Francia

Se encuentra la *Ley número 88-19 de 5 de enero de 1988 sobre el fraude informático*. Entre los delitos de este se pueden mencionar kis siguientes:

- Acceso fraudulento a un sistema de elaboración de datos (462-2). En este artículo se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionario del sistema.[61]
- Sabotaje informático (462-3). En este artículo se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.
- Destrucción de datos (462-4). En este artículo se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que éste contiene o los modos de tratamiento o de transmisión.
- Falsificación de documentos informatizados (462-5). En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.
- Uso de documentos informatizados falsos (462-6). En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.

[61] Ley número 88–19 de Francia, de 5 de enero de 1988 sobre el fraude informático.

3.6.6. Legislación de Portugal

Se hace mención sobre la utilización informática, la cual fue aprobada por la Asamblea Constituyente el 2 de abril de 1976, y la cual expresa en el Artículo 35 sobre "Utilización de la Informática" que señala que[62]:

- Todos los ciudadanos tienen derecho a conocer lo que constare acerca de los mismos en registros mecanográficos, así como el fin a que se destinan las informaciones, pudiendo exigir la rectificación de los datos y su actualización.
- La informática no podrá ser usada para el tratamiento de datos referentes a convicciones políticas, fe religiosa o vida privada, excepto cuando se tratare del proceso de datos no identificables para fines estadísticos.
- Queda prohibida la atribución de un número nacional único a los ciudadanos.

De lo anterior, se advierte que en diferentes países se han preocupado por el mal uso que pueda tener los grandes avances tecnológicos, el cual sin una reglamentación adecuada pueden desbordarse y salir de un control, es así que la apremiante necesidad de que en el Código Penal del Estado, se contemplen de una forma u otra.

La legislación y regulación sobre los delitos informáticos en otros países, constituye un gran avance para países como en el nuestro que no tienen una legislación al respecto, por lo anterior, no se va a realizar una crítica a las anteriores disposiciones legales, ya que cada país contempló dichas normas de acuerdo a sus necesidades propias, como se puede observar en líneas precedentes, (ya que algunos países se enfocaron propiamente a proteger el derecho a la privacidad, y a la propiedad intelectual, o como el que disponga de informaciones nominativas y haga un mal uso de ello; otros tantos a proteger al patrimonio de las personas afectadas como en los fraudes informáticos etcétera). Sin embargo, como se mencionó con anterioridad, ayudan y dan la pauta para que nuestros legisladores contemplen las figuras delictivas de *delitos informáticos*, de acuerdo a nuestra realidad.

[62] La utilización informática, la cual fue aprobada por la Asamblea Constituyente el 2 de abril de 1976.

3.6.7. Legislación de Inglaterra

Computer Misuse Act del año 1990, introdujo el delito de acceso no autorizado. Dice Pacheco Klein que: "Esta cláusula de la ley fue, principalmente, una reacción a la publicidad y al medio en torno a los virus de las computadoras. El artículo 3º inciso 2º establece que la persona tiene que tener intención de "modificar el contenido de cualquier computadora", y de esa manera: Impedir la operación de cualquier computadora; o Impedir o dificultar el acceso a cualquier programa, o la confianza de esos datos. Impedir la ejecución de cualquiera de esos programas, o la confianza en esos datos."[63]

La ley fue criticada por su amplitud, sin embargo la obtención de evidencia desde lugares remotos ha creado problemas en la legislación inglesa.

En 1994, la ley fue reformada para permitir el acceso a la policía y a las agencias especializadas del orden a los boletines informativos.

3.6.8. Legislación de Estados Unidos

Se considera importante mencionar la adopción en los Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) que modificó el Acta de Fraude y Abuso Computacional de 1986[64].

Con la finalidad de eliminar los argumentos hipertécnicos acerca de qué es y qué no es un virus, un gusano, un Caballo de Troya, etcétera y en que difieren de los virus, la nueva acta proscribe la transmisión de un programa, información, códigos o comandos que causan daños a la computadora, al sistema informáticos, 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.

---

[63] Regulación Inglesa: Computer Misuse Act del año 1990.
[64] Revisar la Regulación sobre Delitos informáticos de Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) que modificó el Acta de Fraude y Abuso Computacional de 1986.

El Acta de 1994 diferencia el tratamiento a aquellos que de manera temeraria lanzan ataques de virus de aquellos que lo realizan con la intención de hacer estragos. El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en reclusión federal más una multa y para aquellos que lo transmiten sólo de manera imprudencial la sanción fluctúa entre una multa y un año en reclusión.

Llama la atención que el Acta de 1994 aclara que el creador de un virus no podrá escudarse en el hecho que no conocía que con su actuar iba a causar daño a alguien o que él solo quería enviar un mensaje.

En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo.

En el Estado de California, en 1992 se adoptó la Ley de Privacidad en la que se contemplan los delitos informáticos pero en menor grado que los delitos relacionados con la intimidad que constituyen el objetivo principal de esta Ley.

Es importante destacar las enmiendas realizadas a la Sección 502 del Código Penal relativas a los delitos informáticos en la que, entre otros, se amplían los sujetos susceptibles de verse afectados por estos delitos, la creación de sanciones pecuniarias de $10,000 por cada persona afectada y hasta $50,000 el acceso imprudencial a una base de datos y otros.

El objetivo de los legisladores al realizar estas enmiendas, según se infiere, era la de aumentar la protección a los individuos, negocios, y agencias gubernamentales de la

interferencia, daño y acceso no autorizado a las bases de datos y sistemas computarizados creados legalmente. Asimismo, los legisladores consideraron que la proliferación de la tecnología de computadoras ha traído consigo la proliferación de delitos informáticos y otras formas no autorizadas de acceso a las computadoras, a los sistemas y las bases de datos y que la protección legal de todos sus tipos y formas es vital para la protección de la intimidad de los individuos así como para el bienestar de las instituciones financieras, de negocios, agencias, gubernamentales y otras relacionadas con el estado de California que legalmente utilizan esas computadoras, sistemas y bases de datos.

Es importante aclarar que en uno de los apartados de esta ley, se contempla la regulación de los virus (computer contaminant) conceptualizándose aunque no los limita a un grupo de instrucciones informáticas comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos, modificar, destruir, copiar, transmitir datos y alterar la operación normal de las computadoras, de los sistemas o de las redes informáticas.

CAPITULO IV
TRABAJO DE CAMPO

4.1. OBJETIVO.

Identificar la opinión de los señores entendidos en la materia Penal de delitos Cibernéticos.

4.2. UNIDAD DE ANÁLISIS, POBLACIÓN Y MUESTRA

Unidades de Análisis: en todo planteamiento inicial de investigación es importante establecer quienes son los sujetos u objetos que va a ser motivo de estudio, lo cual requiere definir como un primer paso la definición de la unidad de análisis o también denominada unidades de estudio: son los elemento que van ser medidos o motivo de estudio o investigación.([65])

4.2.1. Población.-

Es el conjunto de elementos finitos que tienen las características comunes y también diferentes que representa la parte de la realidad objeto de investigación o Unidad de Análisis ([66]). En el caso específico esta estará conformada por Fiscales del Ministerio Público, Docentes de la Facultad de Ciencias Jurídicas, Políticas y Sociales en materia Penal e Investigadores de la Fuerza Especial de Lucha contra el Crimen, división Delitos Informáticos.

Es un grupo que representa relativamente en mayor grado todas las características comunes y diferentes de los elementos de la población.([67]) En el caso particular son las personas que acceden y utilizan NTI´s (Fiscales, Investigadores FELCC, Docentes de la

[65] MEJIA IBAÑEZ, Raúl; "Metodología de la Investigación, como realizar y presentar trabajos de investigación"; 3ra. Edición; Artes Gráficas Sagitario; La Paz – Bolivia; 2011;pg.219
[66] MEJIA IBAÑEZ, Raúl; "Metodología de la Investigación, como realizar y presentar trabajos de investigación"; 3ra. Edición; Artes Gráficas Sagitario; La Paz – Bolivia; 2011;pg.134
[67] Ibidem 134

UAP) que totalizan 25 sujetos, que representan el 10% de un total de 250 encuestados que corresponden a un muestreo, no probabilístico.

Para el presente trabajo se utilizará el Muestreo **intencional u opinático**, en el que se utilizan el criterio de un experto o persona de experiencia por medio de la cual se selecciona algunos casos típicos, la muestra procura que ésta sea representativa; en consecuencia, la importancia depende de su intención y por consiguiente es de gran utilidad especialmente en investigación exploratorias, como informantes claves en situaciones específicas.([68])

4.3. MÉTODOS Y TÉCNICAS DE INVESTIGACIÓN.

Para poder recoger la opinión especializada de los señores Fiscales del Ministerio Publico, investigadores de la FELCC. y Docentes de Derecho de la UAP. Los instrumentos para el procesamiento de los datos constaran de cuaderno de notas para el registro de las observaciones y cuadro de observaciones de todas las encuestas realizadas. Finalmente, la información será cotejada e interpretada una vez aplicada un software estadístico para su representación gráfica. El análisis e Interpretación de los datos consistirá en medir el porcentaje de las respuestas para formar un cuadro comparativo de la opinión y realizar la inducción correspondiente.

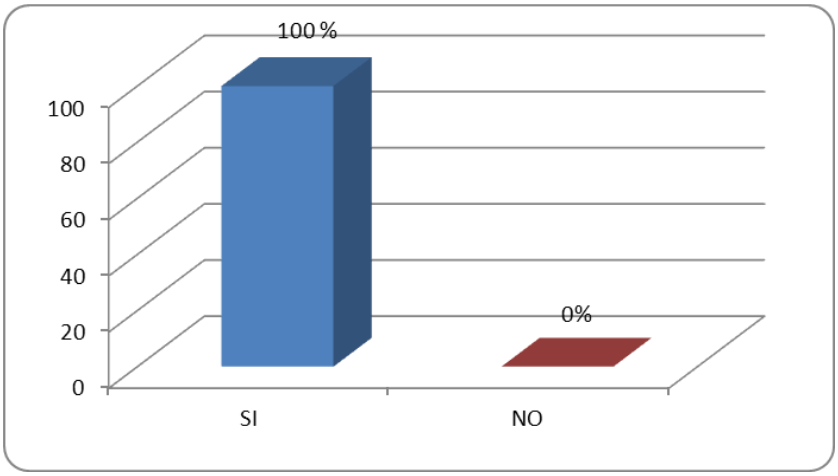
[68] MEJIA IBAÑEZ, Raúl; "Metodología de la Investigación, como realizar y presentar trabajos de investigación"; 3ra. Edición; Artes Gráficas Sagitario; La Paz – Bolivia; 2011;pg.136

4.3.1. Procesamiento y análisis de la información.

Tabla No. 1
¿Conoce Ud. la definición de los delitos informáticos?

INTERROGANTES	%	FRECUENCIA
SI	100	25
NO	0	0
Total	100	25

Gráfica No. 1
¿Conoce Ud. la definición de los delitos informáticos



Análisis e Interpretación:

El 100 % tiene conocimiento de los delitos informáticos; hecho delictivo que afecta los bienes jurídicos protegidos de una forma muy importante.

Análisis:

Se puede determinar, que existe conocimiento adecuado respecto a la definición entre los entrevistados sobre los delitos informáticos, como un hecho que afecta los bienes jurídicos protegidos, de tal manera que debe ser regulada y sancionada. Por lo tanto debe considerarse y constituirse en un elemento central de la propuesta.

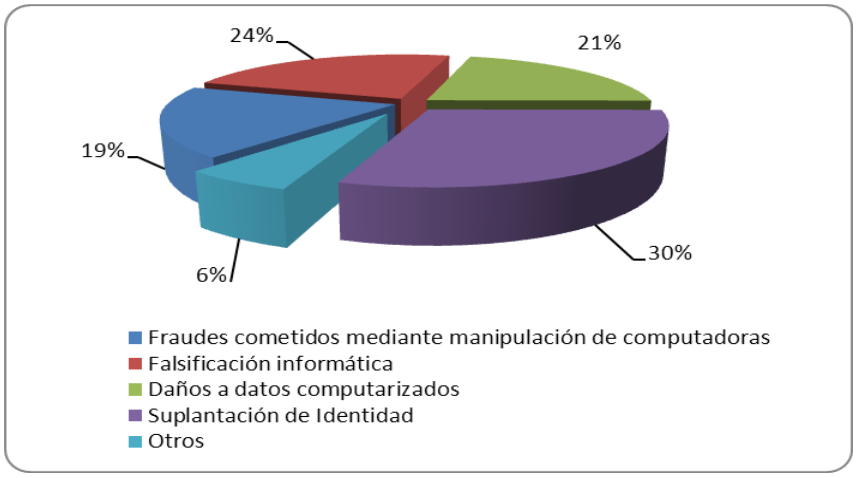
Tabla No. 2

¿Diga Ud. Si conoce algunos de estos delitos informáticos y su importancia y frecuencia?

INTERROGANTES	FRECUENCIA	%
Fraudes cometidos mediante manipulación de computadoras	4,8	19
Falsificación informática	6,0	24
Daños a datos computarizados	5,3	21
Suplantación de Identidad	7,5	30
Otros	1,5	6
TOTAL	25	100

Gráfica No. 2

¿Diga Ud. Si conoce algunos de estos delitos informáticos y su importancia y frecuencia?



Interpretación:

El 30 % Tiene conocimiento de la suplantación de identidad electrónica como un hecho delictivo que afecta los bienes jurídicos protegidos de una forma muy importante y más frecuente. El 24 % tiene conocimiento de la Falsificación informática, que constituye un hecho delictivo que afecta los bienes jurídicos protegidos de una forma importante, El 21% tiene conocimiento de los daños a datos computarizados, como un hecho que afecta a los bienes jurídicos, en el mismo sentido de importancia que en los anteriores casos. El

19 % tiene conocimiento de Fraudes cometidos mediante manipulación de computadoras y El 6 % tiene conocimiento de otros delitos informáticos que afectan a los bienes jurídicos.

Análisis e interpretación de resultados.

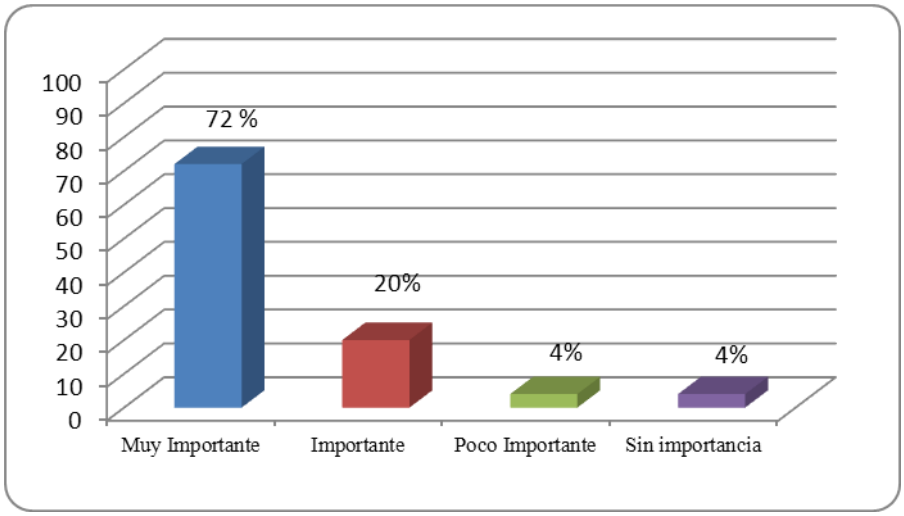
Se puede determinar, que la suplantación de identidad electrónica constituye, entre los especialistas entrevistados el hecho delictivo más conocido y frecuente que afecta los bienes jurídicos protegidos de tal manera que debe ser regulada y sancionada. Por lo tanto su consideración debe constituirse en un elemento central de la propuesta.

Tabla No. 3

¿En su opinión, la regulación expresa de la suplantación de identidad electrónica como un hecho delictivo que afecta los bienes jurídicos protegidos es?

INTERROGANTE	%	FRECUENCIA
Muy Importante	68	17
Importante	20	5
Poco Importante	8	2
Sin importancia	4	1
	100	25

Gráfica No. 3



Interpretación:

El 72% considera que la regulación expresa o combatividad de la suplantación de identidad electrónica es muy importante mientras que El 20% considera que la regulación de la suplantación de identidad electrónica es importante, el 4 % considera esta cuestión o necesidad normativa como poco importante o sin importancia.

Análisis:

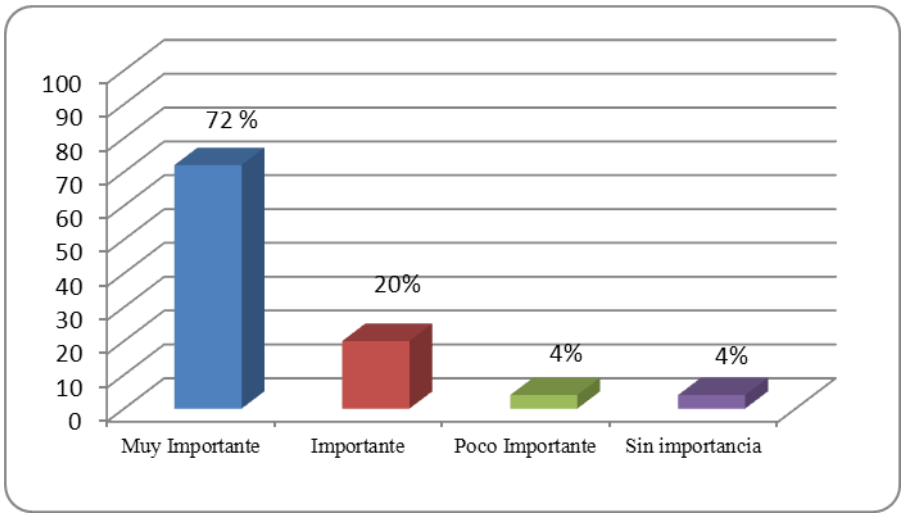
Se puede determinar, que la suplantación de identidad electrónica constituye un hecho delictivo que, afectando los bienes jurídicos protegidos de una forma grave y frecuente, debe ser regulada y sancionada. Por lo tanto su consideración debe constituirse en un elemento central de la propuesta.

Tabla No. 4

¿En su opinión, para la modernización del ordenamiento legal nacional, la complementación de la normativa actual del código penal Sobre delitos informáticos es?

INTERROGANTE	%	FRECUENCIA
Muy Importante	72	18
Importante	20	5
Poco Importante	4	1
Sin importancia	4	1
	100	25

Gráfica No. 4



Interpretación:

El 72% de los encuestados, señalan que la complementación de la normativa actual del código penal sobre delitos informáticos es muy importante, mientras que el 20% señala que la complementación es importante.

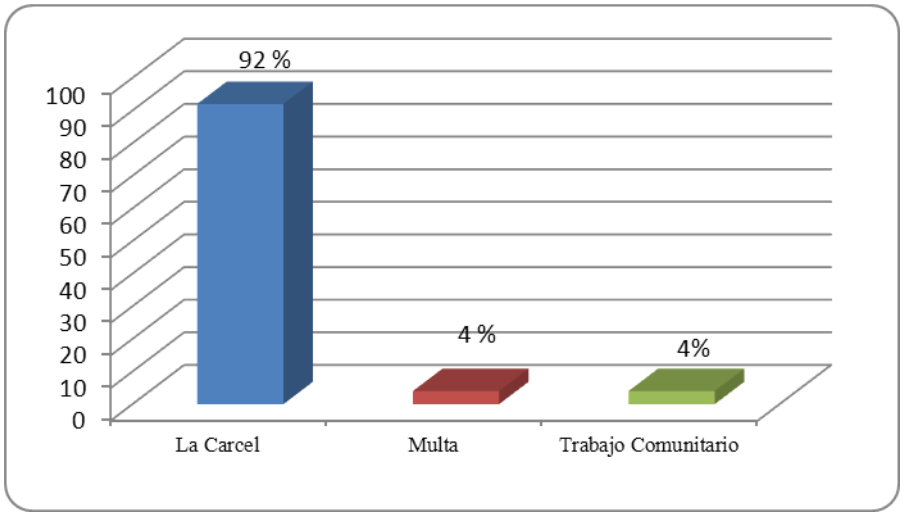
Análisis:

Se puede inferir que la mayoría de los encuestados considera esta situación como una necesidad actual de complementación para la modernización del ordenamiento legal nacional. Por lo que deberá considerarse para su incorporación en la propuesta.

Tabla No. 5
¿En su opinión especializada y de acuerdo a los parámetros de la legislación boliviana cual debe ser la sanción para el delito de suplantación de identidad?

INTERROGANTE	%	FRECUENCIA
La Carcel	92	23
Multa	4	1
Trabajo Comunitario	4	1
	100	25

Grafica No. 5



Interpretación:

Como se ha podido establecer, el 92% de los encuestados, considera que debe sancionarse con la privación de libertad (Cárcel), El 4 % considera que la sanción debe realizarse mediante multa y el 4 % considera que se debe realizar trabajo comunitario como sanción.

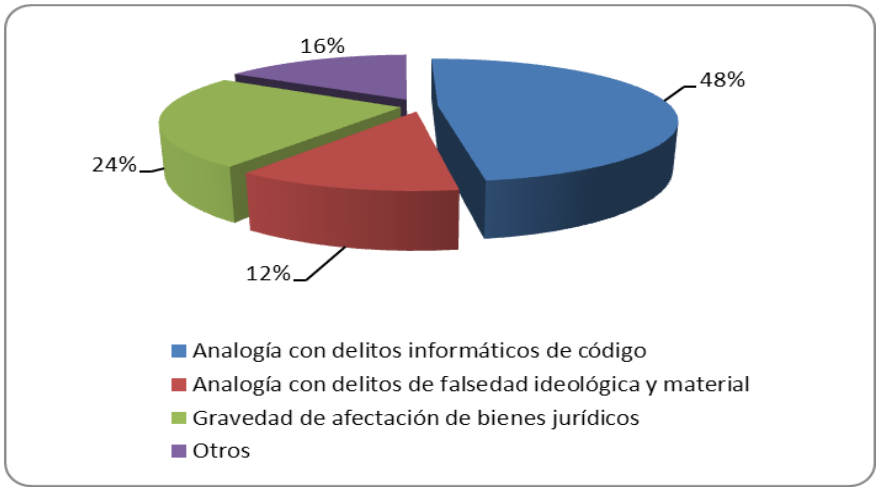
Análisis:

Se trata de una abrumadora opinión respecto a que la sanción debe consistir en pena de prisión, por lo que deberá contemplarse para su inclusión en la propuesta.

Tabla No. 6
¿Cuáles cree usted que deberían ser los parámetros penales para la sanción del delito de suplantación de identidad digital?

INTERROGANTE	%	FRECUENCIA
Analogía con delitos informáticos de código	48	12
Analogía con delitos de falsedad ideológica y material	12	3
Gravedad de afectación de bienes jurídicos	24	6
Otros	16	4
	100	25

Cuadro No. 6



Interpretación:

El 48 % considera que los parámetros penales para la sanción del delito de suplantación de identidad electrónica deben basarse en la analogía con delitos informáticos del código

seguido por un 24% considera que existe una gran afectación a los bienes Jurídicos, seguido por un 16% que consideran otros tipos de delitos penales, y finalmente un 12% considera que deben basarse en la analogía con delitos de falsedad ideológica y material.

Análisis:

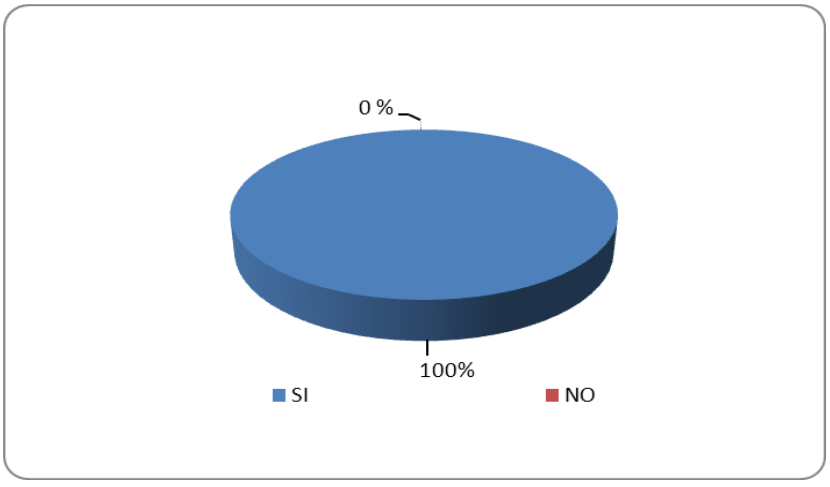
La sumatoria del 24% (gravedad de afectación a bienes jurídicos protegidos) y el 48 % (analogía con suplantación de identidad), confirman la importancia de establecer como criterio fundamental la Analogía con falsedad ideológica complementando con el criterio de gravedad de afectación, debiendo contemplarse para su inclusión en la propuesta.

Tabla No. 7

¿Considera usted que en la era digital y por el grado de afectación de los bienes jurídicos, el delito de suplantación de identidad es más peligroso para la sociedad que otros delitos informáticos aun no tipificados?

INTERROGANTE	%	FRECUENCIA
SI	100	25
NO	0	0
TOTAL	100	25

Cuadro No. 7



Interpretación:

El 100 % de los encuestados, considera afirmativamente esta cuestión, mientras que el considera negativamente el planteamiento realizado.

Análisis:

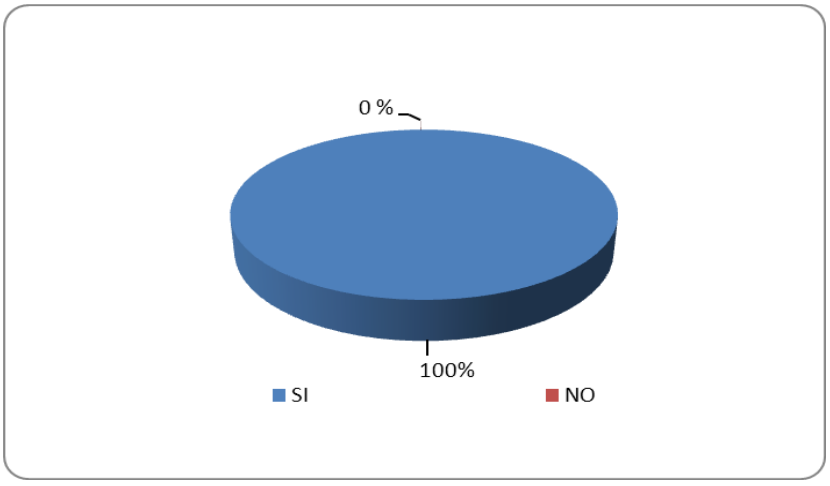
El cuadro demuestra la importancia del problema creado por la peligrosidad de la suplantación de identidad electrónica para los bienes jurídicos protegidos, por lo que deberá considerarse como la base y justificación central de la propuesta.

Tabla No 8

¿Considera usted que, en el marco de la modernización de la legislación penal nacional en la era digital y la protección de los bienes jurídicos afectados, se debe incorporar un artículo sobre suplantación de identidad electrónica en el capítulo correspondiente del Código Penal?

INTERROGANTE	%	FRECUENCIA
SI	100	25
NO	0	0
TOTAL	100	25

Gráfica No. 8



Interpretación:

El 100 % de los encuestados, considera que se debe incorporar un artículo sobre suplantación de identidad electrónica en el capítulo correspondiente del Código Penal.

Análisis:

El cuadro demuestra la importancia de incorporar un artículo sobre suplantación de identidad electrónica en el capítulo correspondiente del Código Penal, por lo que deberá considerarse el objetivo central de la propuesta.

4.4. CONCLUSIONES PARCIALES

Como se puede deducir de los resultados de la investigación empírica realizada, es muy importante incorporar un artículo sobre suplantación de identidad electrónica en el capítulo correspondiente del Código Penal, considerando las necesidades de modernización, complementación de la normativa penal nacional actual y debido al elevado nivel de peligrosidad para los bienes jurídicos que pueden afectarse.

Además, se ha podido establecer cuáles deben ser los lineamientos generales para el tipo de pena y los parámetros temporales correspondientes a la misma, de forma que se cuenta con las bases estructurales generales de la propuesta.

CAPÍTULO V

PROPUESTA
ANTEPROYECTO DE LEY

5.1. DESARROLLO DE LA PROPUSTA

El desarrollo de la tecnología conlleva importantes transformaciones en la sociedad actual, que también se han manifestado en la información y comunicación, cuyos avances tecnológicos han traído variados y múltiples benéficos para la sociedad en todos los ámbitos. Sin embargo, estas tecnologías de información y la comunicación, conllevan además, una serie de factores de riesgo generadores de nuevas conductas delincuenciales a través de dichas tecnologías, por tanto la facilidad para la comisión de este tipo de delitos, como por las dificultades para la presunción penal que tienen estos actos ilícitos. Asimismo la regulación de estos actos es compleja, el rápido avance tecnológico, y la lentitud de los procesos de reforma legislativa, dificulta la labor del derecho penal para regular este tipo de comportamientos de forma oportuna y efectiva. En este sentido, la presente propuesta busca actualizar el marco normativo penal vigente y subsanar uno de los vacios existentes en el ámbito de las tecnologías de la información y la comunicación, a través de la creación de un nuevo tipo penal para la protección de suplantación de identidad, en el área de las tecnologías de la información y comunicación.

Objetivo. Desarrollar el anteproyecto de ley que se compone esencialmente de dos partes. En primer lugar se plantean las bases de la propuesta, el objetivo de la Ley y se definen términos necesarios para su aplicación. En segundo término se plantea la incorporación de un artículo sobre suplantación de identidad al actual Código Penal.

5.2. BASES DE LA PROPUESTA:

Las bases de la propuesta están constituidas, en primer término por la necesidad complementar y modernizar el ordenamiento penal, en el marco de los principios de la carta magna y la evolución del derecho penal a nivel mundial y regional en concordancia

con el avance tecnológico y la aparición de nuevas figuras delictivas. En segundo término, en el ámbito estrictamente del código penal, tenemos un vacío jurídico que atenta no solo al carácter integral de la normatividad del derecho penal nacional si no a los mismos intereses de los la comunidad, cuestiones estas que se han verificado en el marco teórico y el trabajo de campo, y cuyos resultados constituyen las bases directas de la presente propuesta.

Resumiendo los resultados de la investigación podemos establecer que a partir de la expansión globalizada de las nuevas tecnologías de comunicación y comercio electrónico, la suplantación o robo de identidad digital o electrónica, a través de la obtención ilegal de datos personales o claves comerciales, constituye el delito con mayor crecimiento en el mundo y se encuentra asociado a numerosas figuras delictivas como la pornografía infantil, estafas financieras, etc. Considerando que una característica fundamental de este delito es su transnacionalidad y una gran dificultad probatoria, la cooperación internacional es fundamental por lo que la armonización jurídica de las legislaciones nacionales es un prerrequisito para poder combatir eficazmente este delito. Es por ello que desde 2001 la Convención sobre Ciberdelitos de Budapest plantea la necesidad de que las naciones lo tipifiquen como delito.

Si bien nuestro país ha avanzado en materia de delitos informáticos, el robo de identidad digital aún no se considera como delito específico en nuestro ordenamiento penal.

Frente a este contexto, presentamos la presente propuesta en forma de anteproyecto de Ley para llenar el vacío jurídico existente, considerando que la suplantación o robo de identidad debe ser un delito en sí mismo, al margen de la finalidad que persiga, en tanto vulnera ante todo el derecho a la identidad personal, que no se circunscribe a la propiedad de los datos personales de filiación, sino que abarca aspectos de la personalidad de índole cultural, ideológico, religioso o político, que tiene una importancia jurídica en el ámbito de los derechos constitucionales de las personas y los DDHH. Asimismo y como se señaló anteriormente esta figura es utilizada también como medio para cometer distintos tipos de delitos como estafas, abuso infantil amenazas, etc. lo cual lo convierte en un

medio fundamental y altamente peligroso para la comisión de los mismos en la era de la información.

Frente estos nuevos desafíos que provienen del desarrollo tecnológico y la globalización, es necesario actualizar la normativa penal.

5.3. CONSTRUCCIÓN DEL ANTEPROYECTO DE LEY

PROYECTO DE LEY

LEY ESPECIAL DE REFORMA AL CÓDIGO PENAL PARA LA PROTECCIÓN DE LA IDENTIDAD ELECTRÓNICA FRENTE AL DELITO DE SUPLANTACIÓN DE IDENTIDAD EN EL ÁMBITO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN.

Por medio de la cual se modifica el Código Penal, para la protección de la identidad electrónica y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Bolivia: Ley N_____ de_____ de 201____

EVO MORALES AYMA
PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

CONSIDERANDO:

Que la Constitución Política del Estado establece, en su SECCIÓN III ACCIÓN DE PROTECCIÓN DE PRIVACIDAD

Artículo 133

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 y familiar, a su propia imagen, honra y reputación, podrá interponer la Acción de Protección de Privacidad.

Que la Constitución Política del estado establece, CAPÍTULO TERCERO DERECHOS CIVILES Y POLÍTICOS SECCIÓN I DERECHOS CIVILES

Artículo 21. Las bolivianas y los bolivianos tienen los siguientes derechos:

1. A la auto identificación cultural.
2. A la privacidad, intimidad, honra, honor, propia imagen y dignidad.
3. A la libertad de pensamiento, espiritualidad, religión y culto, expresados en forma individual o colectiva, tanto en público como en privado, con fines lícitos.

Que el artículo 25.

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

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

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

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

Que La suplantación de identidad electrónica es una de las actividades ilícitas de más rápido crecimiento en el mundo en tanto que si bien en nuestra legislación existen figuras como el fraude, la falsificación de documentos, u otros delitos informáticos genéricos, la figura de la suplantación de identidad a través de un medio tecnológico no se encuentra tipificada a pesar de que por medio de ella se cometen delitos de diversa naturaleza pero que requieren de esta figura para su comisión.

EN CONSEJO DE MINISTROS,

DECRETA:

Artículo 1.- Objeto de la ley. La presente ley tiene por objeto la protección integral de la identidad electrónica de las personas y de los sistemas que utilicen tecnologías de información, así como la prevención y sanción del delito de suplantación de identidad electrónica cometido contra personas y sistemas mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Artículo 2.- Definiciones. A los efectos de la presente ley, se entiende por:

a. Tecnología de Información: Es la tecnología que lleva a cabo la aplicación y procesamiento de datos, lo cual involucra la obtención, creación, almacenamiento, administración, control, visualización y distribución de información en forma automática, así como el desarrollo y uso del "hardware" y "software" así como todos los procedimientos asociados con el procesamiento de datos.

b. Sistema: Es un conjunto organizado de elementos y procedimientos diseñados para el uso de tecnologías de información, en funciones específicas dentro de unas especificaciones previstas.

Artículo.3 Adiciónese el art. 363 quarter.- al Código penal CAPITULO XI DELITOS INFORMÁTICOS, que quedará redactado de la siguiente manera:

Artículo. 363 quarter.- *Suplantación de Identidad electrónica.* "Será sancionado con privación de libertad":

- de 2 a 6 años el que adoptare, creare, apropiare o utilizare, a través de cualquier sistema informático, o tecnología de Información, red social, sitio de Internet, medio electrónico o tecnológico de información, de la identidad de una persona física o jurídica que no le pertenezca y cause un perjuicio al suplantado de naturaleza física, moral, jurídica o patrimonial.
- La misma pena se le impondrá a quien, utilizando una identidad falsa o inexistente, cause perjuicio a un tercero.

- La pena será de cuatro a ocho años de privación de libertad si con las conductas anteriores se causa un perjuicio a una persona “menor de edad o diferencia de capaciadad”.

Articulo 4 (Disposiciones abrogatorias y derogatorias)

Se abrogan y derogan todas las disposiciones contrarias al presente Decreto Supremo.

Los señores Ministros de Estado, en sus respectivos Despachos, quedan encargados de la ejecución y cumplimiento del presente Decreto Supremo.

Es dado en el Palacio de Gobierno de la ciudad de La Paz, a los…. días del mes de…. del año dos mil trece.

Fdo. EVO MORALES AYMA

CAPITULO VI
CONCLUSIONES Y RECOMENDACIONES

6.1. CONCLUSIONES:

- ✓ Los fundamentos teóricos y jurídicos sobre el derecho informático, los delitos informáticos y de forma especial el de suplantación de identidad electrónica, expuestos y analizados en el marco teórico han permitido establecer la situación, las condiciones generales del objeto de estudio y sus necesidades de desarrollo y complementación.

- ✓ Los resultados del trabajo de campo han permitido identificar y comprobar las dimensiones e indicadores, como solución al problema de investigación a través de la inserción de un artículo sobre la suplantación de identidad electrónica al ordenamiento legal nacional, permitiendo estructurar las bases de la propuesta del presente trabajo de investigación.

- ✓ La propuesta refleja de forma propositiva los resultados de la investigación precedente y fundamentalmente del trabajo de campo, planteando un anteproyecto de ley para la incorporación de un artículo sobre la suplantación de identidad electrónica al ordenamiento legal nacional. En este sentido, la propuesta responde a las necesidades que tiene el derecho penal de armonizar su régimen legal acorde a la realidad nacional y mundial.

6.2. RECOMENDACIONES:

- ✓ A Modo de recomendación general, es necesario que los legisladores tomen conciencia sobre la importancia de este tipo de conductas y se empiece a legislar para que éstas conductas no queden impunes o bien se tipifiquen en otro delito que no es aplicable muchas veces al caso concreto. La legislación penal en nuestro país debe adaptarse a la evolución de la sociedad, y al desarrollo tecnológico actual, por lo tanto debe estudiarse la necesidad de tipificar no solo la suplantación de identidad electrónica sino también a todos los delitos informáticos de acuerdo a la clasificación de la ONU. y las recomendaciones de la convención de Budapest ya sea en una ley especial de informática o la introducción de normas completas y concretas en el Código Penal Boliviano.

- ✓ Existe la necesidad de que la regulación de los delitos informáticos en nuestro país, al margen de lo estrictamente jurídico, reduzca el vacío que existe también en cuanto a la educación y prevención de este delito, por lo que se deben desarrollar campañas de concientización dirigidas a las empresas, organismos, y a la sociedad en general, para dar a conocer las medidas preventivas que se deben adoptar para evitar estas conductas ilícitas incentivando la conciencia de seguridad sobre los sistemas informáticos, ya que son recursos indispensables para la administración de datos en las organizaciones así como para las personas. La seguridad sólo se lograra si se instrumentan los debidos controles tecnológicos o de procedimientos. Asimismo, es necesario desarrollar políticas de regulación para la Protección de Datos Personales en todos los ámbitos sociales.

- ✓ La delincuencia informática crea dificultades para el Derecho Penal Internacional lo que constituye un reto importante para los juristas en busca de lograr eficacia en la prevención y represión de estas conductas. Las diferencias entre las respectivas legislaciones nacionales, como ocurre en el caso de los delitos informáticos, hacen que sea necesario desarrollar una propuesta regional y/o mundial que permita

interactuar a los actores internacionales respetando la jurisdicción de cada país. Respecto a los delitos informáticos se tiene el problema de la extraterritorialidad de las normas, vinculadas a la cuestión de la extradición. Dado el carácter trasnacional de los delitos informáticos es imprescindible establecer tratados internacionales de extradición y acuerdos de ayuda mutua para contrarrestar eficazmente a la criminalidad informática.

- ✓ Se requiere profundizar la capacitación del poder judicial, institución policial, en temas tecnológicos para combatir estos ilícitos sobretodo en relación a la suplantación de identidad vinculada con el fraude financiero y la pornografía infantil, que son los delitos por medios electrónicos que más daño y repudio generan .

- ✓ Conforme al acelerado desarrollo tecnológico de nuestros tiempos se recomienda introducir en la malla curricular universitaria de Derecho de las diferentes universidades del país, al derecho informático.

BIBLIOGRAFÍA CONSULTADA

ALESSANDRI: "La información como bien jurídico" Edit. Albatros. Buenos Aires 2010:

ATHENIENSE, Alexandre, *Auto-Aplicaçao do Código do Consumidor Brasileiro nas Transaçoes de Bens Corpóreos pelo Comércio Electrònico na Internet,* III Congreso de Derecho Informático. Disponible em: http://nombresdedominio.cl, Santiago de Chile 2002. Brasil.

CABANELLAS, Guillermo, *Diccionario Jurídico Elemental. "Derecho Penal"*, Buenos Aires – Argentina. 2000.

CASTELLS, Manuel; "La era de la información: economía, sociedad y cultura", vol. 1, La sociedad Red, Alianza Madrid 1996

CEJA,(Centro de Estudios de Justicia de las Américas) "Perspectivas de uso e impactos de las Tic en la Administración de Justicia en América Latina", www.cejamericas.org, 2008.

CUSICANQUI Morales, Nicolas; "La Pena Legal en Bolivia"; Edito CEDISA La Paz-Bolivia: 2011

DA COSTA RODRIGUEZ, Marco Aurelio Rodriguez**. "***Crimes de Informática"*. Revista electrónica Jus Navegando. Disponible en: www.jus.com.br/doutrina/crinfo.html.

DE LA CUESTA AGUADO, Paz M. (1995). Tirant lo Blanch (ed.); "Tipicidad e Imputación Objetiva", Primera edición;

DICCIONARIO DE LA LENGUA ESPAÑOLA.; Real Academia Española. Madrid - España: Ed. Espasa Calpe. 1992.

GALLEGO HIGUERAS Gonzalo F.; "Código de Derecho Informático y de Las Nuevas Tecnologías", Civitas, Madrid.; 2002

GARCÍA PÉREZ, Inmaculada; "*Derecho Nuevas Tecnologías"*; 14 de Febrero de 2002.

GELHARD, Jorge ; "La evolución del Derecho Penal y los delitos informáticos"; Edit. Mc Graw Hill. México 2011:

GIRALDO, Jaime; "Informática Jurídica Documental"; Temis. Colombia. 1.990.

GUIBOURG, Ricardo A., *Manual de informática jurídica,* Astrea, Capítulo IV – Informática Jurídica de gestión. 1996.

HARVEY, Edwin R, *Derechos de Autor, de la Cultura y de la Información.* Buenos Aires - Argentina: Editorial Depalma, Biblioteca Personal. 1999.

HAWKRIDGE, David; "Informática y Educación. las nuevas tecnologías de la información". Ed. Abeledo- Perrot. Buenos. Aires Argentina, 1992.

HERBAS: Delitos informáticos en Bolivia . Edit ASPROCAP Santa Cruz-Bolivia 2011:

JIJENA LEIVA, Renato Javier: "La Criminalidad Informática": Situación de Lege Data y Lege Ferenda en Chile". Actas de III Congreso Iberoamericano de Informática y Derecho". Mérida, España.

JORDAN FLORES, Fernando; "Las Nuevas Tecnologías, el Derecho y la Justicia", Servigraphic, LTDA, Colombia; 2000.

LEVENE, Ricardo y CHIAVALLOTI, Alicia. "Delitos Informáticos". VI Congreso Iberoamericano Derecho e informática.

MÁRQUEZ; José Antonio, *La contratación electrónica en los códigos civiles*, Cátedra de Informática Jurídica TEC de Monterrey, México. Disponible en: http://www.mty. itesm.mx Junio del 2003. Recuperado el: 15-09-09.

NUÑEZ PONCE Julio, *Derecho informático.* Editores Marsol. El Derecho Informático: concepto y diferencias con la informática jurídica. Autonomía y metodología del Derecho Informático. 2007:

PEÑARANDA QUINTERO Héctor Ramón, **,** (Abogado – Magíster en Gerencia Tributaria – Doctor en Derecho – Presidente de la Organización Mundial de Derecho e Informática – Autor del Libro IUSCIBERNÉTICA: Interrelación entre el Derecho y la Informática, Juez del Tribunal de Protección del Niño y del Adolescente de la Circunscripción Judicial del Estado Zulia) - Maracaibo – Venezuela. 2007: 23

PÉREZ Luño, ENRIQUE Antonio;"Manual de informática y derecho" Editorial Ariel S.A., Barcelona; 1996,

PUCCETTI, Doris Liliana. Revista Notarial. Colegio de Escribanos de la Provincia de Córdoba. Año 1999-1- Nº 77. "El documento electrónico" 1991

REGLAMENTO DEL SOPORTE LÓGICO O SOFTWARE; Jurisprudencia Argentina.- Tomo II- Año 1999- "Documento Electrónico" por Daniel Altmark, págs. 851-855.

RICARDO Levene, y ALICIA Chiavalloti; "Delitos Informáticos". VI Congreso Iberoamericano Derecho e informática.

RODRIGUEZ Sergio; "*Internet y banca electrónica";* Ponencia para despacho Baker & McKenzie. México. Disponible en: http://www.bakernet.com/ecommerce.

SALAZAR Edgar; "*Cibernética y Derecho Procesal Civil*,"; Ediciones Técnico-Jurídicas. Caracas. 1979.

SARZANA Carlos; "El delito informático y su normativa internacional"; Editorial Lozano; Zaragoza España 2009

SONI Mariano, *Compilación de Tratados en Materia de Propiedad Intelectual y Poderes Aplicables en los Países del Continente Americano.* Edición de la Asociación Interamericana de Propiedad Industrial ASIPI. 1995.

TELLEZ Valdez, Julio; "Derecho Informático", Ed. Mc. Graw - Hill México. 1997

UNED. Revista, Iberoamericana de Derecho Informático. XIV Tomos. España. 1.996.

WILLMAN; "Glosas al Código civil Bolivia"; Edit FUNDES. Santa Cruz-Bolivia 2011

BIBLIOGRÁFIA NACIONAL

- Estado Plurinacional de Bolivia Código Penal Edit. Juventud. La Paz-Bolivia 2010.
- Estado Plurinacional de Bolivia Constitución Política del Estado Edit. Juventud. La Paz-Bolivia 2011
- Estado Plurinacional de Bolivia Ley de Telecomunicaciones Edit Juventud . La Paz-Bolivia: 2011
- GACETA OFICIAL DE BOLIVIA; Código Civil Boliviano

BIBLIOGRÁFIA INTERNACIONAL

- 🕮 Regulación Chilena de junio de 1998 por la que se creó la "Comisión Nacional para las Nuevas Tecnologías de Información y Comunicación".
- 🕮 Nota: Se evidencia que en la República de Argentina, los delitos informáticos cuentan con una regulación parcial enfocada más en el campo del Derecho Civil.
- 🕮 El Código Penal del Perú.
- 🕮 Segunda Ley contra la Criminalidad Económica de Alemania del 15 de mayo de 1986, adoptada desde el 1 de agosto de 1986.
- 🕮 Ley de reforma del Código Pena de Austria de 22 de diciembre de 1987.
- 🕮 Ley número 88–19 de Francia, de 5 de enero de 1988 sobre el fraude informático.
- 🕮 El Código Penal de Italia.
- 🕮 La utilización informática, la cual fue aprobada por la Asamblea Constituyente el 2 de abril de 1976.
- 🕮 Regulación Inglesa: Computer Misuse Act del año 1990.
- 🕮 El Nuevo Código Penal Español.
- 🕮 Ley 34 de 11 de julio de 2002.
- 🕮 : Ley Orgánica 15/99 de 13 de Diciembre de Protección de Datos de Carácter Personal.
- 🕮 Revisar la Regulación sobre Delitos informáticos de Estados Unidos en 1994 del Acta Federal de Abuso Computacional (18 U.S.C. Sec. 1030) que modificó el Acta de Fraude y Abuso Computacional de 1986.

WEWGRAFIA

Michel CLAUDIA ARAUJO "Robo de identidad digital: un tema pendiente en la ley boliviana"; http://www.nobosti.com/ spip.php?article1322

OECD: Organización para la Cooperación Económica y el Desarrollo. *Computer related criminalliy: analisys of legal policy in the OECD area*, ICCP, 84:22, 1984. Disponible en: http://www.informatica-uridica.com/trabajos/Criminalidad _informatica_ en_Bolivia

SILVA Neto, Amaro Morales; “Rescatemos los hackers”. Disponible en www.jus.com.br/doutrina/hackers.html

Anexo No. 1

ENCUESTA ELABORADA PARA JUECES Y FISCALES

Nombre y Apellido _____Cargo _____

Tenga la amabilidad de marcar el casillero adjunto a la opción elegida como respuesta a cada una de las preguntas:

1ro. ¿Conoce Ud. Que son delitos informáticos?

SI ☐ NO ☐

2do. ¿Diga Ud. Si conoce algunos de estos delitos informáticos y su importancia y frecuencia?.

Fraudes cometidos mediante manipulación de computadoras ☐
Falsificación informática ☐
Daños a datos computarizados ☐
Suplantación de Identidad ☐
Otros ☐

3ro. ¿En su opinión, la regulación expresa de la suplantación de identidad electrónica como un hecho delictivo que afecta los bienes jurídicos protegidos es?

Muy Importante ☐
Importante ☐
Poco Importante ☐
Sin importancia ☐

4to. ¿En su opinión, para la modernización del ordenamiento legal nacional, la complementación de la normativa actual del código penal sobre delitos informáticos es?

Muy Importante ☐
Importante ☐
Poco Importante ☐
Sin importancia ☐

5to. ¿En su opinión especializada y de acuerdo a los parámetros de la legislación boliviana cual debe ser la sanción para el delito de suplantación de identidad?

La Cárcel ☐

Multa ☐

Trabajo Comunitario ☐

6to. ¿Cuáles cree usted que deberían ser los parámetros penales para la sanción del delito de suplantación de identidad digital?

Analogía con delitos informáticos de código ☐

Analogía con delitos de falsedad ideológica y material ☐

Gravedad de afectación de bienes jurídicos ☐

Otros ☐

7mo. ¿Considera usted que en la era digital y por el grado de afectación de los bienes jurídicos, el delito de suplantación de identidad es más peligroso para la sociedad que otros delitos informáticos aun no tipificados?

SI ☐ NO ☐

8vo. ¿Considera usted que, en el marco de la modernización de la legislación penal nacional en la era digital y la protección de los bienes jurídicos afectados, se debe incorporar un artículo sobre suplantación de identidad electrónica en el capítulo correspondiente del Código Penal?

SI ☐ NO ☐

Anexo No. 2

ENCUESTA ELABORADA PARA INVESTIGADORES FELCC

Nombre y Apellido _____Cargo _____

Tenga la amabilidad de marcar el casillero adjunto a la opción elegida como respuesta a cada una de las preguntas:

1ro. ¿Conoce Ud. Que son delitos informáticos?

SI ☐ NO ☐

2do. ¿Diga Ud. Si conoce algunos de estos delitos informáticos y su importancia y frecuencia?.

Fraudes cometidos mediante manipulación de computadoras ☐
Falsificación informática ☐
Daños a datos computarizados ☐
Suplantación de Identidad ☐
Otros ☐

3ro. ¿En su opinión, la regulación expresa de la suplantación de identidad electrónica como un hecho delictivo que afecta los bienes jurídicos protegidos es?

Muy Importante ☐
Importante ☐
Poco Importante ☐
Sin importancia ☐

4to. ¿En su opinión, para la modernización del ordenamiento legal nacional, la complementación de la normativa actual del código penal sobre delitos informáticos es?

Muy Importante ☐
Importante ☐
Poco Importante ☐
Sin importancia ☐

5to. ¿En su opinión especializada y de acuerdo a los parámetros de la legislación boliviana cual debe ser la sanción para el delito de suplantación de identidad?

La Cárcel ☐

Multa ☐

Trabajo Comunitario ☐

6to. ¿Cuáles cree usted que deberían ser los parámetros penales para la sanción del delito de suplantación de identidad digital?

Analogía con delitos informáticos de código ☐

Analogía con delitos de falsedad ideológica y material ☐

Gravedad de afectación de bienes jurídicos ☐

Otros ☐

7mo. ¿Considera usted que en la era digital y por el grado de afectación de los bienes jurídicos, el delito de suplantación de identidad es más peligroso para la sociedad que otros delitos informáticos aun no tipificados?

SI ☐ NO ☐

8vo. ¿Considera usted que, en el marco de la modernización de la legislación penal nacional en la era digital y la protección de los bienes jurídicos afectados, se debe incorporar un artículo sobre suplantación de identidad electrónica en el capítulo correspondiente del Código Penal?

SI ☐ NO ☐

Anexo No. 3

ENCUESTA ELABORADA PARA DOCENTES UAP

Nombre y Apellido _____Cargo _____

Tenga la amabilidad de marcar el casillero adjunto a la opción elegida como respuesta a cada una de las preguntas:

1ro. ¿Conoce Ud. Que son delitos informáticos?

SI ☐ NO ☐

2do. ¿Diga Ud. Si conoce algunos de estos delitos informáticos y su importancia y frecuencia?.

Fraudes cometidos mediante manipulación de computadoras ☐
Falsificación informática ☐
Daños a datos computarizados ☐
Suplantación de Identidad ☐
Otros ☐

3ro. ¿En su opinión, la regulación expresa de la suplantación de identidad electrónica como un hecho delictivo que afecta los bienes jurídicos protegidos es?

Muy Importante ☐
Importante ☐
Poco Importante ☐
Sin importancia ☐

4to. ¿En su opinión, para la modernización del ordenamiento legal nacional, la complementación de la normativa actual del código penal sobre delitos informáticos es?

Muy Importante ☐
Importante ☐
Poco Importante ☐
Sin importancia ☐

5to. ¿En su opinión especializada y de acuerdo a los parámetros de la legislación boliviana cual debe ser la sanción para el delito de suplantación de identidad?

La Cárcel ☐

Multa ☐

Trabajo Comunitario ☐

6to. ¿Cuáles cree usted que deberían ser los parámetros penales para la sanción del delito de suplantación de identidad digital?

Analogía con delitos informáticos de código ☐

Analogía con delitos de falsedad ideológica y material ☐

Gravedad de afectación de bienes jurídicos ☐

Otros ☐

7mo. ¿Considera usted que en la era digital y por el grado de afectación de los bienes jurídicos, el delito de suplantación de identidad es más peligroso para la sociedad que otros delitos informáticos aun no tipificados?

SI ☐ NO ☐

8vo. ¿Considera usted que, en el marco de la modernización de la legislación penal nacional en la era digital y la protección de los bienes jurídicos afectados, se debe incorporar un artículo sobre suplantación de identidad electrónica en el capítulo correspondiente del Código Penal?

SI ☐ NO ☐

Anexo No. 3

WEWGRAFÍA

DOMINGO laRazón
EL DIARIO NACIONAL DE BOLIVIA

Edición Digital - Domingo, 5 de Junio de 2011

Ciudades

Nueva ley penalizará delitos informáticos

La Razón - Micaela Villa - La Paz

La Ley de Telecomunicaciones, Tecnologías de Información y Comunicación, que está en tratamiento en la Asamblea Legislativa Plurinacional, marcará un punto de inflexión para que se empiece a legislar el derecho informático en Bolivia, se tipifiquen los delitos y se penalicen los delitos.

Marcelo Elío, presidente de la Comisión de Planificación Política, Económica y Finanzas de la Cámara Baja, señaló que es urgente la aprobación de esta norma, porque no existe en este momento un marco legal que proteja los derechos de los bolivianos.
El citado proyecto de ley fue aprobado en grande por esta comisión a finales de mayo.

"Éste es un proyecto para que en Bolivia se empiece a legislar sobre derecho informático, son pautas para iniciar a legislar", dijo Elío.

El proyecto de Ley de Telecomunicaciones menciona en su artículo 116 que se modificarán artículos del Código Penal para sancionar al que incurra en falsedad material, ideológica, de documentos privados, violación de correspondencia y comunicación privada, falsificación y suplantación de identidad electrónica, sabotaje informático, entre otros delitos.

Por el momento el artículo 363 del Código Penal tipifica sólo la manipulación informática y el uso indebido de datos.

"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 cuyo resultado habría sido correcto, ocasionando una transferencia patrimonial en perjuicio de terceros, será sancionado con reclusión de uno a cinco años y con multa de 60 a 200 días".

Con relación al uso indebido de datos, señala: "El que sin estar autorizado se apodere, acceda, utilice, modifique, inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo de hasta un año o multa de hasta 200 días".

Periodista(s): Micaela Villa - La Paz
Es periodista
e-mail: mvilla@la-razon.com

Cambio
Periódico del Estado Plurinacional Boliviano
"La Verdad nos hace libres"
Inicio Noticias Suplementos Staff
Fecha : 2011-05-26

Bolivia penalizará delitos informáticos y digitales

Economía

Comisión legislativa aprobó en grande el proyecto de ley de telecomunicaciones

La Comisión de Planificación, Política Económica y Finanzas de la Cámara de Diputados aprobó ayer, en su estación en grande, el proyecto de Ley de Telecomunicaciones, Tecnologías de Información y Comunicación, que entre otras cosas penaliza el delito informático digital en el país.

Si bien en la actualidad el Código Penal incorpora en el Título X un capítulo destinado a los delitos informáticos, no incluye la descripción de las conductas delictivas en ese orden, lo que debilita la lucha contra estos ilícitos.

Por ello, el proyecto de Ley de Telecomunicaciones plantea la modificación de los artículos 179 bis, 363 bis, 363 ter, 198, 199, 200, 300 y 301 del Código Penal. Las reformas apuntan a vigorizar las penas contra la manipulación informática, la alternación, acceso y uso indebido de datos informáticos y proteger la propiedad intelectual de las obras con soporte electrónico en la web.

Amplía a los delitos de falsedad material, falsedad ideológica y falsificación de documentos privados —que sólo se refieren a instrumentos impresos— en el sistema digital.

Además se sanciona la violación de la correspondencia electrónica privada y la falsificación y suplantación de identidad en la web, que en la actualidad no están tipificadas por la normativa vigente.

Asimismo, el proyecto incluye sanciones privativas que van de tres a seis años a quien cometa sabotaje informático e impida el normal funcionamiento del sistema de información o telecomunicaciones.

DETALLE

En el caso referido a la falsedad ideológica, el proyecto precisa que quien inserte declaraciones falsas en un instrumento público verdadero, será sancionado con privación de libertad de uno a seis años.

Pero la pena se agrava de dos a ocho años de privación de libertad si la persona que cometiere este hecho fuera un funcionario público.

Con relación a la falsificación y suplantación de identidad electrónica en el sistema digital, el proyecto de ley plantea una reclusión de uno a seis años para la persona que incurra en este delito.

La sanción se aplicará en el caso de que una persona altere un mensaje de datos utilizando una identificación física o digital que no le pertenezca y para quien interfiera o altere el proceso de transmisión del mensaje entre los titulares de origen y de destino.

Además se sanciona el delito contra las telecomunicaciones con una pena privativa de cinco años. En este escenario se sanciona a quienes tengan conexiones clandestinas de red, a quien desvíe el tráfico de larga distancia establecido por los operadores y a quien genere tráfico internacional en sentido inverso al normal.

El presidente de la Comisión de Planificación, Política Económica y Finanzas, Marcelo Elío, indicó que una vez aprobada la norma se pondrá en vigencia el documento electrónico y la firma electrónica, lo que permitirá a Bolivia estar a un paso de la emisión de documentos mediante tecnología electrónica, como Internet o las telecomunicaciones digitales, reportó la Cámara de Diputados.

La Comisión parlamentaria aprobó ayer el proyecto en su estación en grande y el legislador anunció la apertura de un ciclo de audiencias públicas para enriquecer los contenidos de la ley.

DOMINGO laRazón
EL DIARIO NACIONAL DE BOLIVIA

Edición Digital - Domingo, 5 de Junio de 2011

Los delitos informáticos se propagan en el país. Las estadísticas proporcionadas a Informe La Razón por la Fuerza Especial de Lucha Contra el Crimen (FELCC) y el Consejo de la Magistratura de La Paz así lo confirman (leer infografías de la otra página). La entidad policial informa que el año pasado recibió 574 denuncias referidas a manipulación informática en ocho departamentos, menos en Oruro. Doce más (casi 2%) que las 562 que llegaron a sus oficinas en 2010.

El director nacional de esta repartición, coronel Jorge Toro, opina que el leve incremento demuestra que, cada día, los delincuentes se apoyan más en las herramientas de la tecnología para realizar actos reñidos con la ley. "Primero se comete el delito (informático), que casi siempre es algo novedoso (para nuestros peritos), mientras la Policía y el Ministerio Público no están debidamente actualizados en el tema y no cuentan con los medios necesarios para combatirlo".

En 2011, el mayor número de casos se registró en Santa Cruz, con un total de 486; seguido por La Paz, donde se presentaron 69. Lo llamativo es que ambas regiones concentran más del 95% de éstos, o sea, 555 de los 574. Posteriormente se ubican Cochabamba, con ocho; Chuquisaca, con cuatro; Tarija, con tres; Beni, con dos, y Pando y Potosí con uno cada uno. Aparte, desde enero hasta marzo de este año ya se suman 47 denuncias en las dependencias policiales.

El artículo 363 bis del capítulo XI del Código Penal dictamina la reclusión de uno a cinco años y una multa de 60 a 200 días para la persona que cometa el delito de manipulación informática. Mientras que el artículo 363 ter sanciona con prestación de trabajo de hasta un año o una multa de hasta 200 días al involucrado en la alteración, acceso y uso indebido de datos informáticos. Sobre este último, la Policía no cuenta con estadísticas.

El panorama se torna más preocupante con el cuadro comparativo proveído por el Consejo de la Magistratura de La Paz, que abarca las causas penales que llegaron a los juzgados de la Corte Superior de Distrito y que fueron extraídas del sistema IANUS, que realiza un seguimiento computarizado de los procesos que se ventilan, y que sirve a los jueces de instrumento para organizar su trabajo y controlar los plazos, con el objetivo de evitar la retardación de justicia.

De 2002 a 2011, los juicios por delitos informáticos crecieron en 890%, de ocho a 79, de los cuales 62 están referidos a manipulación informática y 17, a la alteración, acceso y uso indebido de datos informáticos. Aparte, en esa década, los juzgados paceños recibieron 228 causas referidas al primer delito y 15 del segundo. Asimismo, en los cuatro meses que van de este año, ya se ventilan 29 causas: 27 que incumben al artículo 363 bis y dos al artículo 363 ter del Código Penal.

PESQUISAS. El fiscal de materia Jorge Álvarez comenta que muchos otros hechos relacionados con estos delitos no llegan a ser investigados por las autoridades porque no son denunciados por las víctimas, por desconfianza en el sistema judicial o porque las sanciones son casi simbólicas. “Tiene que ver más con un cambio en la política criminal por parte del Estado, que debería dar hasta 30 años de cárcel y no cinco como en estos casos”. El coronel Toro adiciona que otra razón es el desconocimiento de los damnificados de que hay peritos policiales y del Ministerio Público que averigua estos casos, por lo que recurren a empresas o investigadores privados que cobran por sus servicios.

Por ejemplo, el Instituto de Investigaciones Forenses de la Fiscalía cuenta con equipos para la implementación de la informática forense; su labor empezó hace una década. Pero, desde hace dos años, ante la saturación de trabajo en esta entidad, ocho expertos en el rubro se instalaron en el Instituto de Investigaciones Técnico Científicas de la Universidad Policial, que se organizó sobre la base del exlaboratorio de la Policía Técnica Científica, en el barrio de Següencoma, de la zona Sur de la ciudad de La Paz.

En otros tiempos, este ambiente se dedicaba a indagar exclusivamente hechos delictivos mediante el estudio de las huellas dejadas en la escena del crimen, la balística, la química legal, la toxicología, la accidentología y otro tipo de pericias. Actualmente, su abanico de acción se ha extendido a los delitos informáticos, aparte de pesquisas forenses y de genética aplicativa, explica el jefe de esta dependencia, el capitán William Llanos, quien es titulado en Ingeniería de Sistemas.

El plantel a su cargo recibe las pruebas remitidas desde la FELCC y la Fiscalía. En cuanto a los delitos informáticos, analiza medios electrónicos y ópticos para el almacenamiento de información, sean discos duros de computadoras, CD, DVD, celulares; busca portales de pornografía infantil y realiza patrullajes cibernéticos. “Rastreamos páginas de Facebook o sospechosas que intentan reclutar potenciales víctimas para la prostitución. Así dimos con una página en la urbe de Cochabamba”, indica.

Estos especialistas tratan de involucrarse con el mundo de las redes dudosas del ciberespacio, hacer amistad y socializar con quienes las operan, para atraparlos, posteriormente, con ayuda de los agentes de la FELCC. “Primeramente creamos un perfil que sigue la corriente al delincuente, llegamos a ser parte de sus contactos de confianza y, luego, empezamos a hacer un operativo más complejo que pasa de lo cibernético a lo físico”, que termina en la detención. Y operan de similar modo cuando van tras las pistas de ciberacosadores o chantajistas informáticos.

Generalmente les llega ordenadores que fueron usados para cometer un delito; su dictamen es considerado como parte del cúmulo de pruebas en los juicios. Para los análisis, añade Llanos, precisan conocer la parte tecnológica y su terminología, y también la parte legal. No obstante, a veces, las normas limitan su accionar. Por ejemplo, la Ley de Telecomunicaciones reconoce desde este año la inviolabilidad de los documentos o archivos particulares que están en un ordenador, lo cual está avalado por la Constitución Política, comenta el investigador.

En el ámbito privado, sobresale la empresa Yanapti, inmersa en la averiguación de delitos informáticos, con un laboratorio forense que se halla provisto con equipos y programas especializados que no contaminan la evidencia digital, y que en la mayoría de los casos accede a la información que los criminales depositaron e intentan borrar de sus computadoras, informa Claudia Araujo, abogada y experta en seguridad informática de esta compañía.

RESARCIMIENTO. Araujo agrega, basada en su experiencia y los archivos de casos que residen en su firma, que hay “delitos informáticos cometidos pero que no son descubiertos, otros que se descubren pero no son denunciados y otros que fueron denunciados pero nunca llegaron a una sentencia”. Esto último debido a que en el proceso penal se llega a una transacción entre partes, lo que conlleva, generalmente, el resarcimiento del daño a la víctima, tras lo cual ésta desiste de la demanda y cierra y archiva su expediente.

Más allá de la necesidad de actualización de los delitos informáticos del Código Penal, Milton Mendoza, exfiscal y magistrado suplente del Tribunal Constitucional, espera que con el nuevo Código Procesal Constitucional que pronto será debatido en la Asamblea Legislativa Plurinacional, se abra el principio de

"libertad probatoria" para que los testigos presenten soportes informáticos como pruebas, los cuales —complementa Llanos— deben tener autenticidad, precisión y suficiencia para su validez jurídica.

Hasta ahora, critica Mendoza, hay policías, peritos, fiscales y abogados que aún precisan "capacitación en técnicas, procedimiento e investigaciones nuevas" para garantizar el encarcelamiento de los ciberdelincuentes. Dice ello porque no está enterado de alguna sentencia condenatoria por delitos informáticos; sólo de dos casos pendientes de veredicto en Santa Cruz y otro en Cochabamba. "Un juicio con detención preventiva de los involucrados no es un proceso concluido", resalta el jurista.

Un libro revela los 'hackers' más peligrosos del planeta

Los hackers son los delincuentes o piratas informáticos que vulneran la seguridad de los ordenadores o sistemas electrónicos de personas y empresas, para acceder a información o realizar estafas o robos, entre otros crímenes. Su proliferación va de la mano del auge de los delitos informáticos. Un libro del periodista inglés Misha Glenny, El lado oscuro de internet. La mafia del ciberespacio, devela los nombres de los hackers más avezados y peligrosos del planeta, según la agencia Terra. Entre las historias destaca la de Renukanth Subramaniam, alias JiLsi, quien se sumergió en las aguas de los delitos informáticos y terminó preso por clonar tarjetas de crédito y otros cargos de fraude hipotecario en la red. Los nombres reales y alias de otros hackers famosos son: Adewale Taiwo (Freddybb), Dimitri Golubov, Roman Vega, Maksim Kovalchuk (Blade), Detlef Hartmann (Matrix001), RedBrigade, Max Vision (Max Butler o Iceman), Nicholas Joehle (Dron), Hakim B (Lord Kaisersose), Cha0, Mert Ortaç (SLayraCkEr) y Lord Cyric. Un dato interesante es que el 90% de estos "piratas" quiere trabajar en la industria de la seguridad informática legal.

'Los delincuentes están volando y nosotros, a pie'

Para entender cómo combate la Policía los delitos informáticos o cibernéticos, y cuáles son sus limitaciones, nada mejor que la opinión de quien comanda a nivel nacional la Fuerza Especial de Lucha Contra el Crimen (FELCC), el coronel Jorge Toro, quien señala que su repartición incluso tiene que lidiar con la falta del servicio de internet para investigar estos casos. **— ¿Cuáles son las denuncias más comunes que la FELCC recibe sobre delitos informáticos?**

— Las amenazas por celular se dan a diario y lo único que hacemos es la extracción de los mensajes, no la investigación de dónde provienen, por falta de tecnología.

— ¿Qué es lo que falta para efectivizar el trabajo que realiza la FELCC?

— Nos falta comunicarnos entre las 62 FELCC que operan en el país. Los delincuentes trabajan en red o se mueven de un lugar a otro y nosotros no tenemos ni la instalación de internet, pero inclusive así tratamos de hacer cualquier cosa para poder investigar. Los delincuentes están volando y nosotros vamos a pie.

— ¿Cuál sería la solución?

— Deberíamos implementar un laboratorio de informática actualizado, que costaría alrededor de 20 mil dólares.

— ¿De qué estaría compuesto?

— Básicamente de "clonadores" para extraer de una computadora la información que necesitamos sin contaminarla y así empezar la investigación. Cada uno cuesta 3.000 dólares. Además de un maletín por el cual se pueden ubicar las terminales de todos los celulares, que cuesta alrededor de 8.000 dólares.

También hay herramientas para prevenir los delitos informáticos que son muy difíciles de comprar y de mantener mensualmente. Pero, de acuerdo con las autoridades, hay otras prioridades.

— ¿Las empresas de servicios digitales colaboran con su trabajo de indagación en el caso de las amenazas y acoso por medio de celulares y de internet?

— Todo se trabaja a través de requerimientos fiscales, es decir, que tenemos que esperar entre 15 y 30 días para que nos llegue la información que necesitamos de la empresa privada. En el caso de la información de los IP (números que identifican a un dispositivo en una red), nos llega después de 20 días. Luego de ese tiempo, el malhechor ya se ha escondido o fugado.

— ¿Cómo desarrollan entonces los investigadores su trabajo?

— Muchas veces acuden a la red de internet por sus propios medios, porque no la tienen instalada en la oficina, pero eso no es obstáculo para realizar su labor.

Perfil

Nombre: Jorge Toro Álvarez

Nació: En Villazón, Potosí

Edad: 04-06-56

Profesión: Coronel de Policía con diplomados en Educación Superior, Investigación de las Escenas del Crimen, Anticorrupción, y maestría en Ciencias Forenses

Cargos: Fue perito en el área de Balística y Criminología, jefe de la Policía Técnica Científica, subcomandante de la Unidad de Bomberos, jefe del Departamento Académico de la Universidad Policial. Es Director Nacional de la FELCC


CROSS
CRIME
SCENE