**UNIVERSIDAD MAYOR DE SAN ANDRÉS**

**FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS**

**CARRERA DE DERECHO**

# TESIS DE GRADO

# "LA NECESIDAD DE INCORPORAR EN EL CÓDIGO PENAL EL TIPO PENAL DE FALSIFICACIÓN INFORMÁTICA."

**(Tesis para optar el grado de Licenciatura en Derecho)**

**POSTULANTE:** ROCIO ALEJANDRA TERAN RIVERO

**TUTOR:** DRA. KARINA MEDINACELLI DIAZ

**LA PAZ – BOLIVIA**

**2015**

**DEDICATORIA**

A Dios por darme la luz y la fortaleza necesaria, a mis padres Ruth y Félix por darme la vida, y a mis hermanos Mariela, Marcelo, María Esther, Enrrique y José Cristian porque todos fueron el mejor apoyo en la elaboración de mi tesis.

**AGRADECIMIENTO**

Al plantel docente por inculcarme sus conocimiento, a mi universidad que me abrió sus puertas, y a mi tutora Dra. Karina Medinaceli Díaz, por guiarme en el procedimiento para la elaboración de mi tesis.

**RESUMEN**

El presente estudio se titula: “LA NECESIDAD DE INCORPORAR EL TIPO PENAL DE FALSIFICACION INFORMATICA EN EL CODIGO PENAL”, fue desarrollado por Rocio Alejandra Terán Rivero para optar el grado de licenciada en Derecho, consiste en una investigación a nivel doctrinario con el fin de demostrar la necesidad de incorporar como nuevo tipo penal la falsificación informática en nuestra actual legislación Penal.

A través del desarrollo se explica el constante desarrollo de la tecnología y los vacíos legales dentro de nuestra actual legislación penal con relación a los delitos informáticos, así como también se menciona los artículos que hacen referencia a los delitos informáticos en el Código Penal.

Es preciso entonces una regulación efectiva de la norma penal e incorporar en nuestro Código Penal la falsificación informática debido que existe en nuestro país la necesidad de incorporar nuevos tipos penales para sancionar a aquellos delincuentes que cometen delitos informáticos ya que actualmente no contamos con legislación especifica para tratar este tipo de delitos, también hacer constar que la existencia de la Falsificación Informática como delito informático afecta directamente a un derecho fundamental que es de la información.

Este trabajo es producto de una investigación cualitativa, descriptiva realizada a través de la consulta a la doctrina y legislación vigente nacional y comparada y de las opiniones de profesionales abogados así como Autoridades del órgano Judicial, concluyendo entonces que existen los necesarios y suficientes fundamentos para la incorporación de la Falsificación Informática como nuevo tipo Penal dentro de nuestra Legislación Penal.

**INDICE**

# ***PERFIL***

# ***DE LA***

# ***INVESTIGACIÓN.***

## PERFIL DE LA INVESTIGACIÓN.

### 1.1.- INTRODUCCIÓN

En los últimos años especialmente a raíz del desarrollo tecnológico a nivel mundial se presentaron cambios trascendentales. En este contexto se ha retomado la discusión de la incorporación de nuevos tipos penales dentro de nuestra legislación, convencidos de la necesidad de aplicar con carácter prioritario una política común con objeto de proteger a la sociedad frente a la ciber delincuencia, ya que existe muchos riesgos de que las redes informáticas y la información electrónica sean usadas para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes.

"El delito informático en forma típica y atípica, entendiendo por las conductas típicas, antijurídicas y culpables en que se tienen de forma típica las computadoras como instrumento o fin y por la forma atípica se entiende por delito informático a todas aquellas actitudes ilícitas en que se tienen a las computadoras como instrumento o fin."(1)

En los tiempos actuales se evidencia la necesidad de estudiar nuevas relaciones de la Ciencia del Derecho con las nuevas Tecnologías que van surgiendo periódicamente. Internet es el gran espacio mundial, un espacio virtual, donde se pueden; ofrecer nuestros productos, nuestros servicios, y por tanto es un gran centro comercial, abierto interrumpidamente, es decir sin limitación. La Falsificación Informática es uno de los delitos informáticos con mayor auge en el mundo y consiste en, la introducción, alteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a

[1]TÉLLEZ Valdés, Julio. (1996). pág. 103.

efectos legales, como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles o inteligibles.

### 1.2.- IDENTIFICACIÓN DEL PROBLEMA

En Bolivia, actualmente en nuestra legislación penal vigente existe tan solo dos artículos referentes a los delitos informáticos los cuales son aplicables de manera ambigua a los delitos cometidos por los delincuentes informáticos, en tal sentido genera la necesidad de tipificar nuevos delitos informáticos, conductas antijurídicas, como la falsificación informática, ya que hay muchas conductas que implican responsabilidad para aquellos que lo cometen y es claro que en nuestro Estado existen dos artículos dentro de nuestra legislación penal, el cual hace referencia al mal uso de la Internet, lo cual genera la necesidad de establecer una marco regulatorio modelo para sancionar nuevos tipos penales, efectuando una ampliación al Articulo 363 bis y ter del Código Penal el cual dispone de esta forma:

**ARTICULO 363 bis (MANIPULACIÓN INFORMÁTICA).-** El que con la intención de obtener beneficio indebido para si o para un tercero manipule un procesamiento o transferencia de datos informáticos que conduzcan a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto ocasionando de esta manera una transferencia patrimonial en prejuicio de tercero será sancionado con reclusión de uno a cinco años y con una multa de sesenta a doscientos días.

**ARTICULO 363 ter (ALTERACIÓN ACCESO O USO INDEBIDO DE DATOS INFORMÁTICOS).-** El que sin estar autorizado se apoderare, 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 1 año o multa hasta doscientos días.

En esta parte del articulo 363 bis y ter de nuestra actual legislación penal, señala de manera amplia y ambigua varios tipos penales los cuales incluso tendrían sanciones, sin embargo, haciendo un análisis del artículo, no establece claramente el tipo penal el cual se adecuaría, no es fácil para el legislador aplicar este articulo ya que señala de forma ambigua varias situaciones ni señala el bien jurídico que resguardaría, es inminente la necesidad de incorporar nuevos tipos penales los cuales estén ampliamente desarrollados en nuestro código penal.

En este sentido, la informática puede ser el objeto del ataque o el medio para cometer otros delitos. La importancia reciente de los sistemas de datos, por su gran incidencia en la marcha de las empresas, tanto públicas como privadas, los ha transformado en un objeto, cuyo ataque provoca un perjuicio enorme, que va mucho más allá del valor material de los objetos destruidos.

Al respecto, existen dos grandes grupos de valores merecedores de amparo específico por la legislación penal boliviana.

Por una parte, la criminalidad informática puede afectar a bienes jurídicos tradicionalmente protegidos por el ordenamiento penal, tal el caso de delitos en los que se utiliza la computadora para redactar una carta difamando a personas físicas o jurídicas, o atentar contra la integridad personal, la fe publica o la seguridad nacional.

En otros casos las conductas del agente van dirigidas a lesionar Bienes no protegidos tradicionalmente por la legislación penal, tal el caso de los Bienes Informáticos, consistentes en datos, información computarizada, archivos y programas insertos en el soporte lógico del ordenador, como la falsificación informática, el fraude electrónico y el sabotaje informático.

Existe la necesidad de prevenir y sancionar estos malos usos de la tecnología, y como objetivo principal de la presente investigación es proponer la tipificación del delito informático de falsificación informática en la legislación Penal Boliviana, que tipifique y penalice el mal uso de los sistemas informáticos de tal forma que se sancione la falsificación informática, ya que cada día aparecen nuevos métodos de vulneración de los sistemas informáticos.

### 1.2.1 PROBLEMA CENTRAL

¿Qué razones explican la necesidad de incorporar el tipo penal de Falsificación Informática en el Código Penal?

### 1.2.2. PROBLEMAS SECUNDARIOS.

¿Cuál la naturaleza jurídica del Delito Informático?

¿Cuáles las características origen y evolución del delito informático?

¿Es viable la incorporación de la falsificación informática en el Código Penal?

## 1.3.- DELIMITACIÓN DEL TEMA.

### 1.3.1.- Delimitación Temática.

La investigación se circunscribe al análisis jurídico, dogmático y de derecho comparado de la figura del delito de falsificación informática abarcando el área del Derecho Penal y el área del Derecho Informático**.**

### 1.3.2.- Delimitación Temporal.

La investigación se desarrolla en base a la normativa actual vigente en nuestro país y la situación del delito informático en el Derecho Penal en los seis meses anteriores.

### 1.3.3.- Delimitación Espacial.

La investigación se circunscribe al análisis jurídico dela incorporación de la falsificación informática bajo la normativa Penal en Bolivia. Por lo que las entrevistas a realizarse es para recoger información primaria de profesionales abogados y jueces del área penal de La Paz.

## 1.4.- FUNDAMENTACIÓN E IMPORTANCIA DEL TEMA DE TESIS.

La importancia del tema de la presente tesis radica principalmente que desde el punto de la eficacia jurídica de una norma, explicar la necesidad de incorporar en el Código Penal el tipo penal de falsificación informática a efectos de generar recomendaciones para crear una norma eficaz para la misma sociedad, es de vital importancia determinar los fundamentos para la aplicación de dicha norma la cual es necesaria para todos los ámbitos de la sociedad, en especial en el ámbito de la seguridad de la información, es decir si dicha norma es viable. Y más importante aún es determinar las razones de su viabilidad y/o inviabilidad a fin de que la norma goce del equilibrio social y jurídico requerido para su aplicación eficaz.

Por otro lado el estudio de los delitos informáticos tiene gran importancia puesto que ha a pesar de pertenecer y estar regulado en una norma especifica cómo es nuestro actual Código Penal, en nuestro país debido a la ambigüedad del Artículo 363 bis y ter ni si quiera contaríamos con un bien jurídicamente protegido el cual este desarrollado en dicho artículo.

Este es el marco que justifica la investigación a realizarse y resumiendo se tiene que la importancia del tema es:

a. Desde una perspectiva jurídica: seguridad jurídica.
b. Desde una perspectiva normativa: de fundamentación de la introducción de la norma que respalda su eficacia y validez.

## 1.5.- OBJETIVOS DE EL TEMA DE TESIS.

### 1.5.1 Objetivo General.

Establecer la necesidad de incorporar en el Código Penal el tipo penal de la falsificación informática, para tal efecto identificar su naturaleza y fundamento jurídico para proponer recomendaciones que determinen una norma eficaz.

### 1.5.2. Objetivos Específicos.

1. Describir características origen, concepto y evolución de los Delitos Informáticos.
2. Analizar la teoría del delito sus caracteres y componentes con relación a los delitos informáticos.
3. Determinar específicamente la legislación penal vigente acerca de delitos informáticos.
4. Describir el concepto y la clasificación de la falsificación informática.

## 1.6.- HIPÓTESIS DE TRABAJO.

La incorporación de la falsificación informática como tipo penal en Bolivia, permitirá una mayor protección al bien jurídicamente protegido de la información**.**

### 1.6.1 VARIABLES.

#### 1.6.1.1. DEPENDIENTE.- EFECTO.-

Permitirá una mayor protección al bien jurídicamente protegido de la información.

#### 1.6.1.2 INDEPENDIENTE.- CAUSA.-

La incorporación de la falsificación informática como tipo penal en Bolivia.

### 1.6.2. UNIDADES DE ANÁLISIS

La unidad de análisis es:

La eficacia de la tipificación de los Delitos Informáticos.

### 1.6.3. NEXO LÓGICO

El nexo lógico de las variables señaladas es PERMITIRÁ.

## 1.7.- MÉTODOS Y TÉCNICAS A UTILIZAR EN LA TESIS.

La investigación se enmarca en el tipo descriptivo y cualitativo.

Es de tipo descriptivo porque…"se analizan las variables de la hipótesis planteada tal como está, sin manipular ningún factor que las afecte"(2).

Y es de carácter eminente cualitativo es decir…"para verificar hipótesis en grupos pequeños para llegar a profundizar la investigación,"(3)porque con el objetivo de incorporar la falsificación informática en el Código Penal la información a obtenerse tiene mas valor por su calidad que por su cantidad al ser un estudio jurídico.

### 1.7.1. MÉTODOS.

#### 1.7.1.1. OBSERVACIÓN SISTEMÁTICA.

Es un método que permitirá sistematizar las observaciones realizadas en la documentación obtenida acerca de los Delitos Informáticos asimismo se sistematizara la información obtenida tanto en fuentes primarias o secundarias.

[2] PAREDES Ana Maria (2008) Pág. 62

[3] PAREDES Ana Maria (2008) Pág. 62

### 1.7.1.2. MÉTODO DEDUCTIVO

"Se partirá de un conjunto de teorías conceptos los cuales validaran la hipótesis de investigación."( 4 ) Se utiliza por cuanto con base a esta sistematización de la información se deducirá y sintetizará el papel de los Delitos Informáticos en nuestro Código Penal, así como la incorporación de la falsificación informática.

### 1.7.1.3. MÉTODO INDUCTIVO.

Se aplica en el análisis de la información obtenida de fuentes primarias a través de entrevistas realizadas a profesionales abogados y jueces del área penal, sobre los fundamentos que apoyan o rechacen la incorporación de la falsificación informática, induciendo las conclusiones a que se lleguen del procesamiento de tales entrevistas siendo así…"partir de lo particular para llegar a lo general**."(5)**

## 1.8. TÉCNICAS A UTILIZARSE EN LA TESIS.

### 1.8.1. TÉCNICA DE REVISIÓN DOCUMENTAL.

Se utilizara para la obtención de información de fuentes secundarias, con la realización de fichas bibliográficas por tema de la información obtenida en libros, documentos memorias e informes y la revisión de información en documentos publicados, en Internet sobre el tema tratado en los países elegidos con legislación similar a la de nuestro país.

### 1.8.2. LAS ENTREVISTAS.

"La entrevista como técnica de investigación, los cual precisan para contrastar la hipótesis,"( 6 ) se realizara a dos universos, como a profesionales abogados y jueces del área penal permitiéndonos recopilar la

[4] PAREDES Ana Maria pág. 33

[5] PAREDES Ana Maria pág. 33

[6] PAREDES Ana Maria Pág. 106

información necesaria, para una mejor comprensión de la presente investigación, para lo cual se estructurara una guía cuestionario de preguntas cerradas o abiertas.

# ***MARCO TEORICO***

## CAPITULO I

## 1.-MARCO HISTÓRICO

### 1.1.- EVOLUCIÓN DE LOS DELITOS INFORMÁTICOS

Nuestro país de una economía basada principalmente en la industria petrolera, minera y agrícola, con una área industrial muy reducida en comparación con otros países, concentra un significativo sector de la población dedicado a la administración del estado; que necesariamente debe estar capacitado en el manejo de ordenadores o computadoras, ya que la informática se constituye en una herramienta imprescindible en la actualidad para el correcto y eficaz funcionamiento tanto de las instituciones estatales como de las instituciones privadas Actualmente la informática es una herramienta imprescindible para el correcto y eficaz funcionamiento de las instituciones públicas como privadas.

"Los avances de las tecnologías de la información, comunicaciones y el crecimiento de las operaciones comerciales mediante un medio electrónico han propiciado el surgimiento de nuevas conductas fraudulentas relacionadas con el uso de instrumentos electrónicos."(7)

Sin embargo, el uso de la informática en nuestro país no es privativo, debido a la baja de ordenadores y de procesadores coloca a grupos importantes de nuestra población a estar en contacto con la tecnología generando diferentes actividades así como redes sociales, correo electrónico e incluso juegos electrónicos. Las medidas del estado como la entrega gratuita de ordenadores a bachilleres de nuestro país, la instalación de 2000 antenas Wi Fi, en el área rural para internet, así como telefonía

[7]RICO Carrillo Marilina (2013) pág. 208.

móvil sumándose también la compra del satélite TUPAC KATARI, así como el crecimiento de nuestras empresas de telefonía las cuales están en constante actualización de tecnología, por estos motivos es necesario la necesidad de contar con una ley específica acerca de delitos informáticos la cual este acorde con el desarrollo de la tecnología.

En nuestro país los delitos informáticos no solo están ligados con las instituciones, sino que están ligados también con el desarrollo de la población y en si de la sociedad ya que al desarrollo de las tecnologías, nuestra sociedad se encuentra vulnerable ante nuevas formas de delitos cometidos mediante ordenadores, cajeros automáticos tarjetas de crédito etc.

"Los primeros estudios empíricos sobre el delito informático fueron realizados a mediados de la década de 1970, si bien estos estudios sacaron a la luz un limitado número de delitos, simultáneamente indicaron fuertemente que un gran número de estos delitos permanecían sin descubrirse o sin denunciarse. La perspectiva publica y científica acerca de los delitos informáticos cambio radicalmente en los ochenta, una amplia ola de piratería de programas, manipulación de cajeros automáticos y abusos de las telecomunicaciones revelo la vulnerabilidad de la sociedad de la información y la necesidad de nuevas estrategias de control de estos delitos."(8)

Creemos que, en la actualidad, es innegable la existencia de delitos cometidos mediante el uso de instrumentos informáticos ..."más aún, mediante el análisis de las normativas existentes en el derecho

[8]SAEZ Capel José. (2014) pág. 57.

comparado,"(9) de donde surge la necesidad de estructurar un nuevo bien jurídico digno de tutela jurídica penal, que entendemos y sostenemos que se trata de la información en todas sus etapas, la cual conlleva en sí un valor, ya sea económico, ideal o de empresa como veremos más adelante, que es relevante y digno de tutela jurídico penal.

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robos, hurtos, fraudes, falsificaciones, perjuicios, estafas, sabotajes. Sin embargo, debe destacarse que el uso de las técnicas informáticas han creado nuevas posibilidades del uso indebido de las computadoras lo que ha creado la necesidad de regulación por parte del derecho. Este tipo de delitos son considerados un aspecto negativo del desarrollo de la informática y se producen debido a las posibilidades que las computadoras ofrecen para infringir la ley.

"En este contexto, aparecen conductas que vulneran bienes jurídicos no convencionales, o comportamientos que se realizan empleando medios no convencionales para lesionar bienes jurídicos convencionales."( 10 )La regulación jurídica de la criminalidad por o contra el ordenador presenta determinadas peculiaridades debidas al propio carácter innovador que las tecnologías de la información y la comunicación presentan. Son evidentes e indiscutibles los beneficios de la informática en la comunidad. Empero, los aspectos negativos comprenden inimaginables formas de cometer delitos. En el plano jurídico - penal, la criminalidad informática puede suponer una

[9] Legislación de EEUU, Alemania, Francia, Argentina, Chile, entre otras que iremos estudiando en el transcurso de la investigación.

[10] BOTELO Candia G. [en línea] http://publicaciones.derecho.org/redp/index.cgi?/N%Famero_4__julio_de_1999/001. [Consulta 30/07/14..]

nueva versión de delitos tradicionales o la aparición de nuevos delitos impensables antes del descubrimiento de las nuevas tecnologías.

Así, como las nuevas tecnologías nos traen destacables ventajas, es importante responder eficientemente a la necesidad de regular las conductas que pueden derivarse del uso indebido de las tecnologías siendo de esta forma el uso indebido de ordenadores, de tarjetas de crédito y débito.

A los efectos de lograr un mayor abundamiento en la investigación a desarrollar, como también una clara y ordenada explicación de la misma, tomaremos distintos parámetros para elaborar un esquema acerca de la evolución de los delitos informáticos:

- "En los años 1970 y siguientes fueron los europeos los primeros países en tomar conciencia de los avances de la informática, los cuales generarían mayores peligros, con relación al bien jurídicamente protegido, en los años setenta se referían al ámbito de la intimidad."(11)
- Entre 1970 y 1980, se comenzó a regular el tratamiento de datos personales mediante ordenadores, tanto en Suecia, Alemania así como también en EEUU. Comienza así, la inclusión de diversas normas penales en los ordenamientos europeos a los efectos de proteger la privacidad y la confidencialidad, sin embargo en los años ochenta a delitos se desarrollaron delitos informáticos de contenido económico y se resguardaba la propiedad intelectual de los programas.
- A partir de 1980 comienza un proceso legislativo originado en Estados Unidos luego se extendió a Europa como reacción de la

[11] SAEZ Capel José. (2014) pág. 178.

legislación tradicional que solo protegía los bienes materiales. Se legisla sobre protección de bienes intangibles dinero electrónico, soportes informáticos, etc.

- En los años 1980 y 1990 por su importancia económica, se incluye a los programas informáticos, como obras protegidas por el Derecho de Autor. Los separa en otra sección, distinguiéndolos en protección para semiconductores, y para las bases de datos y los secretos comerciales.
- A partir de 1986 en diversos países se van desarrollando Reformas en el Derecho Penal para combatir esta nueva forma de delitos generando seguridad y derecho
- En los años noventa al desarrollo de nuevos paradigmas reguladores del derecho a la información.

## 1.2. DELITO INFORMÁTICO EN LA DOCTRINA

En ocasiones las referencias a los hechos delictivos relacionados con la informática se realiza mediante la expresión o denominación de delito informático expresión que posee cierto atractivo por su simplicidad, …"por responder a la terminología anglosajona computer crime en realidad se trata de un concepto ambiguo que ni posee ningún sentido estricto con ninguna categoría jurídico penal con un exclusivo hecho punible de los previsto en el Código Penal."(12)

"En países de nuestro entorno socio- cultural hace ya tiempo que el delito informático está tipificado y como tal incluido en diferentes Códigos y norma de su ordenamiento."(13) El área informática dentro de la Doctrina, sostiene que, no pueden penalizarse conductas que atenten contra supuestos bienes

[12] MATA Ricardo (2001) pág. 21.

[13] DAVARA Rodriguez M.A. (2008) PAG. 351.

jurídicos que no se encuentran protegidos, y que no habiendo ley que tipifique una conducta delictiva relacionada con la informática como bien jurídico específico, no existe delito ni pena para dichas conductas. Existen otras posturas que entienden que debe existir algún tipo de protección contra dichas conductas, o más bien, una ampliación en la interpretación sobre ciertas conductas antijurídicas ya tipificadas, en base a las nuevas modalidades perpetradas utilizando sistemas tecnológicos avanzados como los sistemas informáticos o telemáticos en la actualidad, es innegable la existencia de delitos cometidos mediante el uso de sistemas informáticos. Más aún, mediante el análisis de las normativas existentes en el derecho comparado, de donde surge la necesidad de estructurar un nuevo bien jurídico digno de tutela jurídica penal, que entendemos y sostenemos que se trata de la información en todas sus etapas, la cual conlleva en sí un valor, ya sea económico, ideal o de empresa.

### 1.3 CARACTERES

Pasemos ahora a definir los caracteres del delito informático. A nuestro entender, quién mejor los establece es el jurista mexicano Julio Téllez Valdéz quién desarrolla en forma específica las siguientes características:

1). Son conductas criminales de cuello blanco, porque sólo un determinado número de personas con ciertos conocimientos técnicos puede llegar a cometerlas.
2) Son acciones ocupacionales, porque en muchas veces se realizan cuando el sujeto se halla trabajando.
3) Son acciones de oportunidad, porque se aprovecha una ocasión creada o altamente intensificada en el mundo de funciones y organizaciones del sistema tecnológico y económico.
4) Provocan serias pérdidas económicas.

5) Ofrecen posibilidades de tiempo y espacio, ya que en milésimas de segundo y sin una necesaria presencia física pueden llegar a consumarse.
6) Son muchos los casos y pocas las denuncias, y todo ello debido a la misma falta de regulación por parte del Derecho.
7) Son muy sofisticados.
8) Presentan grandes dificultades para su comprobación, esto por su mismo carácter técnico.
9) En su mayoría son imprudencias y no necesariamente se cometen con intención.
10) Ofrecen facilidades para su comisión los menores de edad.
11) Tienden a proliferar cada vez más, por lo que requieren una urgente regulación.(14)

## 1.4 TIPOS DE DELITOS INFORMÁTICOS

La siguiente tabla esquematiza los principales tipos de delitos informáticos la cual muestra un panorama de la siguiente manera:

| | | |
|---|---|---|
| **Robos hurtos, vaciamientos, desfalcos estafas o fraudes cometidos mediante manipulación y uso de computadoras.** | Manipulación de los datos de entrada– insiders | fraude informático conocido también como sustracción de datos, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir. |

[14]TELLEZ Valdez Julio. (1996) pág. 104 y ss.

| | | |
|---|---|---|
| | La manipulación de programas | Consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas. Ej: Caballo de Troya, |
| | Manipulación de los datos de salida-outsiders | 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. . |
| | Fraude efectuado por manipulación informática | aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salami" en la que cantidades de dinero muy pequeñas, se van sacando repetidamente de una cuenta y se |

| | | |
|---|---|---|
| **Fraudes contra sistemas, daños o modificaciones de programas o datos computarizados.** | | transfieren a otra. |
| | Sabotaje informático | Consiste en borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Ejsvirus, gusanos, rutinas cáncer, bomba lógica. |
| | Acceso no autorizado a sistemas y servicios. | Motivos diferentes curiosidad, (Hacker) hasta el sabotaje o espionaje informáticos son ingresos no autorizados comprometen la integridad y la confidencialidad de los datos. |
| | Espionaje – Acceso telemático no autorizado a un sistema - Hackers – Fuga de datos. | Es la obtención de información para ser utilizada posteriormente normalmente para la obtención de beneficios económicos Ejs Puertas |

| | | |
|---|---|---|
| **Falsificaciones informáticas.** | | falsas, pinchado de líneas, llave maestra (Supperzapping). |
| | Reproducción no autorizada de programas informáticos piraterías. | Ley Nº 17.616 promulgada el 13 de enero de 2003 Ley de Protección del Derecho de Autor y Derechos Conexos, la cual modifica el texto de la ley 9.739. |
| **Datos personales delito de violación a la intimidad.** | Como objeto | Cuando se alteran datos de los documentos almacenados en forma computarizada. Pueden falsificarse o adulterarse también micro formas, micro duplicados y microcopias esto puede llevarse a cabo en el proceso de copiado o en cualquier otro momento. |
| | Como instrumentos | Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso |

| | | |
|---|---|---|
| **Homicidio.** | Violación de la intimidad de la vida personal y familiar ya sea observando escuchando o registrando hechos palabras, escritos o imágenes, valiéndose de instrumentos procesos técnicos u otros medios. | comercial. Las fotocopiadoras computarizadas en color a base de rayos láser dio lugar a nuevas falsificaciones. |
| **Interceptación de comunicaciones (browsing)** | Es posible cometer homicidio por computadora ej un paciente que esta recibiendo un determinado tratamiento, se modifican las instrucciones en la computadora que puede hacerse incluso desde una terminar remota. | |
| **Robo de servicios** | | |

| | | |
|---|---|---|
| | Mediante la conexión en paralelo de terminales no autorizados se puede acceder a datos e incluso manipular la información | |
| **Hurto calificado por transacciones electrónicas de fondo.** | Robo de servicios o Hurto de tiempo de ordenador. | Los empleados utilizan en una empresa horas de maquina sin autorización para realizar trabajos personales. |
| **Delitos de daño aplicable al hardware** | Apropiación de informaciones residuales . | Apropiación de informaciones que han sido abandonadas por sus legítimos usuarios de servicios informáticos como residuo de determinadas operaciones . |
| | Parasitismo informático. | Se alude a las conductas que tiene por objeto el acceso ilícito a los |

| | | |
|---|---|---|
| | | equipos físicos o a los programas informáticos, para utilizarlos en beneficio del delincuente. |
| | Este es el caso del hurto que se comete mediante la utilización de sistemas de transferencia electrónica de fondos de la telemática en general, o también cuando se viola el empleo de claves secretas. | Un ejemplo es el referente al uso ilícito de tarjetas de crédito |
| | El robo de un establecimiento comercial de una o varias computadoras no constituye un delito informático, pero si el daño o sabotaje al hardware que combate la puesta en marcha de un sistema | |

| | | |
|---|---|---|
| | informatizado de diagnostico medico. Puede darse un atentado contra la maquina o sus accesorios (discos, cintas terminales etc.) | |

**FUENTE: VIEGA Maria Jose 182 a 186.**

## 1.5. DELITOS INFORMÁTICOS

Así, como las nuevas tecnologías nos traen destacables ventajas, es importante responder eficientemente a la necesidad de regular las conductas que pueden derivarse de su uso indebido. Los delitos informáticos son considerados un aspecto negativo del desarrollo de la informática y se producen debido a las posibilidades que las computadoras ofrecen para infringir la ley. En este contexto, aparecen conductas que vulneran bienes jurídicos no convencionales, o comportamientos que se realizan empleando medios no convencionales para lesionar bienes jurídicos convencionales. Empero, los aspectos negativos comprenden inimaginables formas de cometer delitos. En el plano jurídico penal, la criminalidad informática puede suponer una nueva versión de delitos tradicionales o la aparición de nuevos delitos impensables antes del descubrimiento de las nuevas tecnologías. Por tratarse de un sector sometido a constantes fluctuaciones e innovaciones tecnológicas, sus categorías son asimismo efímeras y cambiantes. Además, los delitos informáticos se caracterizan por las dificultades que entraña descubrirla, probarla y perseguirla, a ello se añade la facilidad de penetrar en los sistemas informáticos.

### 1.5.1. CONCEPTO DE DELITOS INFORMÁTICOS.

Es necesario realizar un concepto sobre los llamados delitos informáticos. Al respecto, se han formulado en doctrina diferentes denominaciones para indicar las conductas ilícitas en las que se usa la computadora. Existe diferentes conceptos acerca de los delitos informáticos, a continuación citaremos algunos autores que se refieren a los delitos informáticos de la siguiente manera:

"Jimena Leyva define a los delitos informáticos como: toda acción típica antijurídica y culpable para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma."(15)

Miguel Ángel Davara Rodríguez señala que …"la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardware o software"(16)

El Convenio de Ciberde lincuencia del Consejo de Europa de 23 de noviembre del 2001 llevado a cabo en Budapest, define los delitos informáticos como …"actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, así como el abuso de dichos sistemas, medios y datos."(17)

Las Naciones Unidas, conceptualiza a los delitos informáticos como "todos los delitos cometidos por medio de tecnologías de información; en contra de

[15] VIEGA MariaJose (2003) pag. 178.

[16] DAVARA RODRIGUEZ M.A. (2008) pág. 350

[17] CONVENIO DE CIBERDELINCUENCIA Budapest (2001) pág. 15.

cualquiera de sus componentes o los que fueren cometidos por medio de tecnologías de información."(18)

Julio Téllez Valdés conceptualiza …"delito informático de forma típica y atípica, entendiendo a la primera como las conductas típicas, antijurídicas y culpables, en las que se tienen a las computadoras como instrumento o fin y a las segundas actitudes ilícitas en que se tienen a las computadoras como instrumento o fin."(19)

Ricardo M. Matta y Martin define al delito informático como "toda acción dolosa que provoca un perjuicio a personas o entidades, en cuya comisión intervienen dispositivos habitualmente utilizados en las actividades informáticas."(20)

Los delitos informáticos en sentido estricto vendrían a ser todo comportamiento ilícito que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin, para llevar a cabo actos ilícitos, esta es una visión limitada porque existen muchos delitos que no pueden tipificarse con las leyes vigentes y, ante la ausencia de una normatividad acorde, se habla de lagunas o de falta de regulación.

## 1.6 SUJETOS Y RELACIONES QUE SURGEN DEL DELITO INFORMÁTICO

### 1.6.1. SUJETO ACTIVO

"El sujeto activo de los delitos informáticos, puede ser cualquier persona abarca tanto a particulares como funcionarios públicos,"(21).El sujeto activo simplemente encuentra la manera de ingresar a la información o contenido del área protegida en si ingresa a los sistemas operativos como un intruso,

[18] NACIONES UNIDAS (2000) pag. 4.
[19] TÉLLEZ Valdés, J. (1996). págs. 103 - 104.
[20] MATTA Y MARTIN Ricardo (2001) pag. 21.
[21] SAEZ Capel Jose (2014) pág. 234

vulnerar sistemas de seguridad es un reto personal en si el sujeto activo de los delitos informáticos tienen habilidades especificas para el manejo de los sistemas informáticos.

"Es evidente que el nivel de aptitudes del delincuente informático es hoy un tema de controversia, ya que para algunos estudiosos del tema, dicho nivel 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 pueden encontrarse en un empleado del sector de procesamiento de datos de cualquier organización". (22)

Los sujetos activos de los delitos informáticos tienen las siguientes características:

a) Poseen importantes conocimientos de informática.
b) Ocupan lugares estratégicos en su trabajo, en los cuales se maneja información de carácter sensible se los denomina delitos ocupacionales ya que se cometen por la ocupación que se tiene y el acceso al sistema.
c) A pesar de las características anteriores debemos tener presente que puede tratarse de personas muy diferentes. No es lo mismo el joven que entra a un sistema informático por curiosidad, por investigar o con la motivación de violar un sistema de seguridad como desafío personal, que el empleado de una institución financiera que desvía fondos de la cuentas de los clientes.
d) Las opiniones en cuanto a la tipología del delincuente informático se encuentran divididas, ya que algunos dicen que el nivel educacional a

[22]LEVENE, Ricardo, CHIARAVALLOTI, Alicia. "Introducción a los Delitos Informáticos, Tipos y Legislación". (en línea) http://www.chiaravalloti_asociados.dtj.com.ar/links_1.htm Consulta en 30/07/14.

nivel informático no es indicativo, mientras que otros aducen que son personas inteligentes, motivadas y dispuestas a aceptar el desafío tecnológico.

e) Estos delitos se han calificado de cuello blanco, porque el sujeto que comete el delito es una persona de cierto estatus socioeconómico."(23)

Al desarrollar todas estas características, es evidente que el sujeto activo de los delitos informáticos son personas que conocen los sistemas operativos así como conocen como vulnerar dichos sistemas y usar de manera ilícita la información ya se información personal de algún usuario o información institucional de empresas públicas o privadas.

"Es de destacar que la cifra negra de delitos informáticos es muy alta. No es fácil descubrirlos ni sancionarlos. Los daños económicos son altísimos. Se habla de pérdidas anuales por los delitos informáticos y otros tecno-crímenes que van de se los U$S 100 millones hasta la suma de U$S 5.000 millones, estos datos de acuerdo a un estudio realizado a finales de los años 1990 hecho por una firma auditora."(24)

### 1.6.2 SUJETO PASIVO

"El sujeto pasivo son aquellos sobre los que recae la acción u omisión que realiza el sujeto activo."(25)en realidad el sujeto pasivo es la víctima del delito es el sujeto en el cual recae la acción u omisión que realiza el sujeto activo, las víctimas pueden ser individuos, instituciones crediticias, instituciones militares, gobiernos, instituciones bancarias etc., que usan sistemas automatizados de información, generalmente conectados a internet.

[23]VIEGA M.J. (2003) pág. 180 - 181.
[24] VIEGA M.J. (2003) pág. 181.
[25] VIEGA M.J. (2003) pag. 181.

“En el caso el sujeto pasivo es el titular del sistema u ordenador intrusado incluso muchas veces a los proveedores de servicios públicos, sistemas financieros y casos hay de algún servicio de inteligencia de una gran potencia.”(26)

El sujeto pasivo pueden ser desde una familia, individuos, empresas grandes y pequeñas, instituciones públicas privadas, instituciones bancarias, gobiernos, que utilizan sistemas automatizados de información, los cuales, por lo general se encuentran conectados a internet. La condición relevante a cumplir por el sujeto pasivo, es la de poseer información en formato digital y almacenada en un medio informático pueden ser datos, programas, documentos electrónicos, dinero electrónico, información, etc, y que se encuentra en contacto directo con la tecnología, específicamente con las redes de Internet.

## 1.7. PERFIL CRIMINOLÓGICO

“Las tecnologías de la información han facilitado la aparición de nuevas conductas que con independencia del mayor o menor reproche social generado, han obligado a los países avanzados a adaptar sus legislaciones para dar cabida a modalidades comisivas que no existían hace unos años.”(27)

Existen diferentes tipos de perfil de delincuentes informáticos y se clasifican de la siguiente manera:

a) Hacker Persona que disfruta explorando detalles de los sistemas programables y aprendiendo a usarlos al máximo, al contrario del operador común, que en general, se conforma con aprender lo básico

[26] SAEZ Capel Jose (2014) pág. 235

[27] RIVAS Alejandro J.(1999) pag 134.

actúa por curiosidad…."Con el termino hacking nos referimos a la técnica consistente en acceder a un sistema informático sin autorización. Entendemos que existe autorización cuando el sistema esta conectado a una red pública y no dispone de un control de acceso mediante el uso de identificadores de usuario y pasword accediendo a información confidencial del usuario."(28)

b) Cracker Aquel que rompe con la seguridad de un sistema, hablar de…"craks nos referimos a los programas o rutinas que permiten utilizar o inutilizar los sistemas de protección establecidos por el titular de los derechos de propiedad intelectual sobre una aplicación informática."(29)

c) Preaker Es aquella persona que intercepta la red telefónica para obtener beneficios personales, "preacking entraría en las técnicas de fraude en materia telefónica analógica y digital."(30)

d) Phisher…"es aquella persona que se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas."(31)

Habiendo expuesto el concepto de delito informático, y en razón de no extendernos en temas que serán tratados en otros puntos de la presente

[28]RIVAS Alejandro J.(1999) pag 135
[29]RIVAS Alejandro J.(1999) pag 134.
[30]RIVAS Alejandro J.(1999) pag 135.
[31]Wikipedia "phishing" ( en línea) es/Wikipedia.org/wiki/phishing. Consulta 18/07/14.

investigación, pasaremos a desarrollar la teoría del delito con relación a los delitos informáticos.

**RESUMEN ANALÍTICO**

Habiendo desarrollado características, tipos de los delitos informáticos y en si habiendo conceptualizado de manera clara que es el delito informático y habiendo recurrido a varios autores y desarrollando los sujetos los cuales participan dentro de estos delitos podemos aclarar que el delito informático para nosotros se define como cualquier conducta criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin, para llevar a cabo actos ilícitos.

Por tanto al no tener una tipificación completa de los delitos informáticos acudiremos al conocido principio de nullum crimen nullapoena, sine lege, no existe crimen sin una ley e indicaremos que no habiendo ley que tipifique y consecuentemente indique la conducta delictiva y no habiendo ley que la determine cuál es la pena, no existe delito ni pena por la acción por dolosa que fuere. Es necesaria la creación de nuevos tipos penales en nuestra legislación Penal para esta clase de acciones jurídicamente reprochables.

Sin embargo cabe aclarar lo siguiente que no es la computadora la que atenta contra el hombre, es el hombre el que encontró una nueva herramienta, quizás la más poderosa hasta el momento, para delinquir, no es la computadora la que afecta nuestra vida privada, sino el aprovechamiento que hacen ciertos individuos de los datos que ellas contienen.

La humanidad no está frente al peligro de la informática sino frente a individuos sin escrúpulos con aspiraciones de obtener el poder que significa el conocimiento. Por eso la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas.

# ***MARCO REFERENCIAL***

## CAPITULO II

### 2.1. EL DELITO INFORMÁTICO Y LA TEORÍA DEL DELITO

En el presente punto haremos un breve análisis a la luz de la Teoría del Delito, sobre los caracteres esenciales que fuimos desarrollando en los puntos anteriores, como configuradores específicos del delito informático. En varios de ellos, y en orden a la temática expuesta, hemos realizado dicho análisis en puntos anteriores, por lo tanto en esos casos, sólo haremos referencia al análisis desarrollado en los mismos.

En esta óptica, el derecho penal, se ha visto transformado en sus formas y ámbitos de intervención. Aparecen en conductas que emplean medios no convencionales para la comisión de hechos ilícitos creándose problemas en el momento de su sanción. El impacto de la explosión tecnológica es un problema que la política criminal conoce sobradamente. La técnica siempre es un arma y cada avance fue explotado criminalmente, en forma tal que siempre el criminal está más tecnificado que la prevención del crimen. En este sentido para desarrollar la teoría del delito es necesario conceptualizar al delito como …" una acción típicamente antijurídica y culpable, de acuerdo a ella los elementos constitutivos del delito son acción tipicidad, antijuricidad y culpabilidad."(32)

"La Teoría del Delito es una teoría de la aplicación de la ley penal, y como tal pretende establecer un orden para el planteamiento y la resolución de los problemas que implica la aplicación de la ley penal, en materia penal esto encuadra a lo que se conoce como tipo que define y establece los elementos del delito." (33) La misma cumple una doble función mediadora, por un lado entre la ley y la solución del caso concreto y por otro lado, una mediación

[32] MIGUEL HarbBenjamin (2003) pag. 178.
[33] MIGUEL HarbBenjamin (2003) pag 259.

entre la ley y los hechos que son objeto del juicio. Se denomina así al estudio del conjunto de elementos del delito considerados como partes autónomas, mediante las cuales es posible aprender el concepto unitario, aunque complejo, de la infracción punible, por tanto ningún acto humano puede ser reprochado como delito, sí una ley no lo prohíbe previamente, para ello, es necesario comprobar que alguien se comportó de la manera prevista en la ley, que dicho comportamiento no se encontraba autorizado en las circunstancias en que tuvo lugar, y por último, que el autor de dicho comportamiento tenía las condiciones personales requeridas para poder responsabilizarlo por la conducta realizada. De esta tripartición problemática de la aplicación de la ley penal, surgieron las conocidas categorías de origen alemán que hoy designamos como acción, tipicidad, antijuridicidad y culpabilidad,…"todo el derecho penal vigente se inspira en el principio nullum crimen nullapoena sine lege, no hay delito, no hay pena , sin ley previa que surge contra la arbitrariedad para que nadie sea juzgado por cualquier conducta sin que ella este definida en el Código Penal y para que nadie arbitrariamente se a condenado a penas que no consignen la ley para el delito incriminado."(34)

Ahora analizaremos estos elementos desde la óptica particular de la temática, objeto de la presente investigación.

### 2.1.1. EL PRINCIPIO DE LEGALIDAD

El Principio de Legalidad, exige como condición esencial, la existencia de un régimen jurídico que formule la descripción del hecho o conducta criminal y de la pena a imponerse, previamente al hecho que califica a ella como criminal, para imputar a una persona como autora del delito. La concreción

[34] MIGUEL HarbBenjamin, (2003) pág. 94.

legislativa de nuevos supuestos de incriminación que supongan nuevos delitos, es un paso importante para llevar a cabo en nuestra legislación.

Si bien, y como ha quedado demostrado en los puntos anteriores, a nivel mundial existen varios pronunciamientos y reformas legislativas tendientes a la protección de bienes jurídicos o intereses como ser el software, la información, la intimidad, etc, debemos remarcar que dicha nueva normativa, brinda una solución parcial a la problemática que nos ocupa. “Por ello, ante determinadas situaciones, sería conveniente contemplar situaciones puntuales de violación a los sistemas informáticos, a través de figuras tipo, contempladas en los Códigos Penales.”(35)

Es de vital importancia comprender el principio de legalidad para así tener mas clara la necesidad de contar con una normativa clara y evidente acerca de los delitos informáticos en la cual se individualice nuevos tipos penales.

“En nuestro país en los que respecta a la materia penal específicamente las fuentes de conocimiento es decir, las formas o modos de manifestación de voluntad de la autoridad que posee la facultad de dictar la norma jurídica son inmediatas o primarias, o sea que tienen vigencia obligatoria por sí mismas, y en nuestro sistema jurídico, la única fuente inmediata de conocimiento es la ley penal.”(36).

Para no extendernos en la explicación de cada una de las consecuencias, que son conocidas por todos, sólo trataremos aquellos puntos que puedan arrojar un poco de luz a la temática planteada. .

[35]CREUS, Carlos. (2004) pág. 45 .
[36]CREUS, Carlos. (2004). págs. 51 y ss.

“Las leyes de esta especie se mantienen en el marco de la legalidad represiva exigida por la división de los poderes, mientras que su complemento se establezca por una ley en el sentido constitucional, o un acto administrativo, cuyo objeto de regulación.”(37)

Más allá de la discusión sobre la conveniencia o no del dictado de este tipo de normas, creemos que es necesaria la actuación legislativa en esta específica materia. Es decir, a pesar del contenido fluctuante de las conductas antijurídicas o anómalas perpetradas mediante medios informáticos, resulta necesario el dictado de leyes que específicamente aborden dicha temática, más aún contando con la experiencia de otras naciones para el análisis e interpretación de éste tipo de actos delictivos.

### 2.1.2. PRINCIPIO DE RESERVA PENAL

Como mencionamos al inicio del punto anterior, el Principio de Reserva Penal, se encuentra en la garantía de la legalidad. Es decir, que el ámbito de lo punible debe estar determinado exhaustivamente por la ley, y que todo lo que queda al margen de ese ámbito está reservado como esfera de impunidad.

“El Principio de Reserva presupone como condiciones de su existencia, las siguientes: La determinación legal de los hechos punibles, la determinación legal de las penas correspondientes, la prohibición de la analogía y la irretroactividad de la ley penal.”(38)

Al respecto, creemos que ya ha sido analizada, en los puntos anteriores, la problemática de los delitos informáticos, en relación al principio de reserva penal. Sólo resta aclarar que la garantía individual está antes del derecho

[37]NUÑEZ, Ricardo C. (1987). pág 81
[38]NUÑEZ, Ricardo C. (1987), pág 83

penal: se refiere a la facultad de actuar del hombre dentro de lo permitido39, sin que su conducta pueda acarrearle sanción alguna. O sea que es una garantía del individuo, no directamente ante los organismos de "persecución", sino ante el mismo órgano de legislación penal: este no puede asignar una pena a una conducta que esté permitida por el ordenamiento jurídico, antes tiene que prohibirla.

La doble garantía del principio de reserva (una limita la libertad de punir, y la otra la de prohibir), tienen una especial importancia en el análisis de las nuevas figuras delictivas en el ámbito de la informática. Debemos considerar – especialmente en nuestra legislación actual -, la necesidad de distinguir entre software y hardware; siendo el primero el elemento lógico del sistema informático (programas), y el segundo el elemento material (maquinaria, aparatos, etcétera).

Y dicho esto, el elemento lógico por su naturaleza jurídica, escapa a la esfera de protección penal común, necesitando una tutela especial cuando las acciones punibles son realizadas mediante la ejecución de medios de tecnología computacional.

Para concluir, volvemos sobre algo antes mencionado, y es la necesidad de crear tipos específicos que involucren conductas antijurídicas o anómalas, cometidas mediante sistemas informáticos, y con la determinación de las penas que correspondan a cada una de ellas.

[39]CREUS, Carlos. (2004). pág. 55.

## 2.2. CONSIDERACIONES GENERALES SOBRE LA CONFIGURACIÓN DEL ILÍCITO INFORMÁTICO A LA LUZ DE LA TEORÍA DEL DELITO.

En este punto analizaremos algunos aspectos a tener en cuenta en la configuración del ilícito informático, en base a lo sostenido por la Teoría del Delito.Como ya mencionamos, el delito es considerado como …"una acción típicamente antijurídica y culpable, de acuerdo a ella los elementos constitutivos del delito son acción tipicidad, antijuricidad y culpabilidad"(40) y cuando se infringe voluntariamente este deber, nos referimos a la culpabilidad. El derecho penal se refiere a delitos y no al delito, el tipo lo concebimos según nuestro derecho como la visualización general de la característica de la conducta propuesta para la pena. (41)

Por lo tanto pasaremos a desarrollar cada una de las partes constitutivas del delito en relación a nuestra investigación.

### 2.2.1. LA ANTIJURIDICIDAD

"Hemos dicho que el delito es la conducta típicamente antijurídica y culpable de ello resulta que la antijuridicidad es un concepto genérico del delito sin ella no hay delito" (42)…"la ilicitud se encuentra ubicado antes que el tipo penal"( 43 ), porque éste designa sólo conductas que ya son antijurídicas. Sin entrar en la discusión doctrinaria sobre la ubicación antes o después del tipo de la antijuridicidad, creemos que para el análisis de los ilícitos informáticos, los cuales se encuentran sin tipificación correcta en nuestro Código Penal, es conveniente realizar la primera medida, una investigación sobre la licitud o ilicitud de dichas conductas según el

[40] MIGUEL HarbBenjamin(2003) pag. 178.
[41]CREUS, Carlos. (2004) págs. 55 y ss
[42] MIGUEL HarbBenjamin (2003) pag. 273.
[43] MORALES Guillen Carlos. (1993) pág. 24.

ordenamiento general. …" de modo general lo antijurídico es lo contrario al derecho."(44)

La antijuricidad es un juicio de valor que recae sobre un comportamiento humano contrario a la exigencia de un ordenamiento penal, es decir lo antijurídico es todo lo que va en contra de las mismas leyes.
"La ley penal sólo puede formular esa valoración sobre conductas que ya se encuentran jurídicamente desvaloradas."(45)

En la materia que nos ocupa, existe un gran número de conductas cometidas mediante sistemas informáticos, que si bien a nivel internacional, ya han sido desvaloradas, a nivel nacional o regional, no han sido catalogadas dentro de esa categoría, o se encuentran en análisis por parte del ordenamiento general.
Es por esto que tomamos, la postura de analizar la antijuridicidad, como presupuesto del tipo, y no como la contradicción de la conducta con el plexo normativo, ya que en varios supuestos dicho plexo no existe, o se encuentra en vías de existir.

Sentado lo anterior se sostiene…"que los medios informáticos alteran los esquemas tradicionales de interacción social, y ofrecen nuevas formas de relación entre las personas."(46) Como consecuencia de lo antedicho, se desprende el hecho de que además, sirven como medios de comisión de delitos ya tipificados en la mayoría de los códigos penales, además de que pueden generar violaciones de bienes jurídicos protegidos, cuya vulneración, hasta la fecha no se considera delito, pero que en el consciente popular,

[44] MIGUEL HarbBenjamin (2003) pag 273.
[45] CREUS, Carlos. (2004). págs. 148.
[46] CAMPOLI, GABRIEL Andres. (2003). pág. 8.

violan al menos las reglas de normal convivencia pacífica en sociedad, pilar del carácter tuitivo de las ciencias penales.

De esto resulta obvio, que no necesariamente todas las conductas posibles deriven directamente en conductas criminalizadas, pero, lo que nadie puede negar, es que al menos algunas de estas nuevas conductas posibles deberían ser incluidas en los Códigos vigentes tal como lo han hecho a la fecha algunos ordenamientos a nivel nacional e internacional.
El problema de esta actitud, radica principalmente en el hecho de que …"la sociedad rara vez espera los cambios legislativos para modificar sus conductas, más bien ésta y su realidad concreta suelen estar varios pasos delante de legisladores y juristas."(47)

Es por esto, que necesariamente, el legislador penal, ha de tener en cuenta los nuevos fenómenos informáticos como también los cambios de orden sociológicos que el mismo trae aparejado, debe capacitarse al respecto, a los fines de poder otorgar un valor jurídico-penal a un hecho perpetrado mediante sistemas informáticos hacia bienes protegidos o dignos de protección penal.
Y esto se dificulta aún más, a la hora de establecer lo que desea evitar la norma primaria, o sea lo que tiene el hecho de antijurídico (lo esencial de la prohibición)en los ilícitos cometidos a través de Internet.

Todo esto se debe, claramente al hecho de que si bien los individuos existen en ella como entidades autónomas, singulares e irrepetibles,…"la despersonalización física que permite la red hace casi imposible el ejercer sobre ellos coerción física o aún en algunos casos hasta jurídica a la vista de

[47]CAMPOLI, GABRIEL ANDRES. (2003). pág. 10.

que los derechos nacionales no poseen la jurisdicción y competencia necesarias."(48)

### 2.2.2. ACCIÓN U OMISIÓN DEL DELITO.

Pero, también creemos que es posible, cometer delito de omisión dentro de la especie de delitos informáticos. Aclaramos que no hemos visto regulado en forma específica lo que no significa que en algún país efectivamente se haya regulado de dicha manera algún delito informático perpetrado por omisión.

Al respecto, proponemos el siguiente análisis de una conducta que bien puede tomarse como un delito por omisión. Se trata del caso del operador de un sistema informático en una organización determinada, que maneja información protegida, que omite actualizar el antivirus de su ordenador, ante un inminente ataque a su ordenador. "El resultado de la omisión es dejar el mundo exterior tal cual estaba antes, en este caso todo cambio, ya que la información puede bien haber sufrido un daño (parcial o total), dicho daño puede ser irreparable, o bien se configuró un delito de peligro hacia dicha información, como bien protegido, ya que existió probabilidad de daño, o sea que no se consumó la lesión del bien jurídico, sino que con el solo hecho de poner en peligro a dicho bien, se configura el delito."(49)

### 2.2.3. TIPICIDAD

En relación a la tipicidad, es importante aclarar la necesidad actual, tanto nacional como a nivel mundial, de tipificar la mayor cantidad de conductas que puedan configurar delitos informáticos. En este sentido, mencionamos en forma precedente, los esfuerzos a nivel mundial, de organismos internacionales, como también de los Estados parte de sistemas de integración regional, en lo que respecta a esta preocupación legislativa.

[48] CREUS Carlos. (2004). pág. 185.

[49] GARCÍA RIVAS, NICOLÁS.(2002)pág. 136.

Si bien existen países cuya legislación se encuentra muy avanzada al respecto existen determinados elementos de los delitos informáticos, como también del medio, mediante el cual se perpetran dichos ilícitos, que hacen que dicho esfuerzo sea más loable de realizarse en conjunto.

Adoptar políticas conjuntas en lo que hace a seguridad, ya sea en el uso de Internet, como así también en el comercio electrónico, o en tráfico de datos, es indispensable para lograr un efecto integrador de los instrumentos de control social, a nivel mundial. Además, también encontramos actitudes ilícitas que jurídicamente ya están configuradas como delitos en el ordenamiento penal, pero estimamos que la legislación debe perfeccionar debido al vertiginoso desarrollo que viene alcanzando el uso de la tecnología informática.

"Dichos delitos nos llevan a adoptar nuevos criterios sobre el tipo, ya que el mismo cuando se realiza pues genera una actividad ilícita."(50)

### 2.2.4. CULPABILIDAD

"Se afirma por muchos autores que la culpabilidad es un juicio de reproche por la ejecución de un hecho contrario a lo mandado por la ley."(51)

En el ámbito de la culpabilidad, el Derecho tiene dos formas para hacer responder al sujeto por sus acciones.

"Por un lado tenemos la responsabilidad objetiva. En este caso, el sujeto responde porque su acción menoscabó un bien jurídico (el derecho pretende volver a equilibrar las relaciones de bienes que la acción desequilibró). Por

[50] CREUS, Carlos. (2004). pág. 183.

[51] MIGUEL HarbBenjamin (2003) pág. 308.

otro lado, tenemos el caso de la responsabilidad subjetiva."(52) Aquí, el sujeto responde porque la acción se le puede reprochar por haber actuado con voluntad de desconocer el mandato protector del bien jurídico. Aquí el reproche se presenta como fundamento o presupuesto de la sanción. Al mundo de la responsabilidad objetiva pertenece la Teoría del Delito.

Ahora bien, habiendo seguido este pequeño esbozo realizado por el autor citado, y sin entrar en el debate sobre el contenido de la Teoría de la Culpabilidad y su ubicación, sólo haremos referencia a algunas consideraciones a tener en cuenta relacionadas al tema que nos ocupa.

En primer lugar, debemos aclarar que sólo serán delitos aquellas conductas que se tipifiquen como tales en virtud del principio de legalidad. Segundo, es conveniente que solo las conductas más graves y preferentemente dolosas, se castiguen penalmente, dado el carácter de última ratio, de último recurso de la pena dentro del sistema de control social. Es decir, que solo una vez que las medidas sancionatorias civiles, y administrativas han sido descartadas, las sanciones serán las penales.

En segundo lugar, y volviendo a lo mencionado respecto a la responsabilidad subjetiva, habíamos dejado sentado, que en dicho caso, el sujeto responde porque la acción se le puede reprochar por haber actuado con voluntad de desconocer el mandato protector del bien jurídico, ya sea queriendo violarlo o por no atender como hubiese debido a la posibilidad de violarlo.

Sin embargo, al hablar de delitos informáticos y culpabilidad existe un problema en nuestro país, al momento incluso de denunciar una situación en la cual exista un ilícito informático, primero por la falta de tipificación de

[52]NUÑEZ, Ricardo C. (1987). pág. 89.

tipos penales, segundo por la falta de una unidad especializada en la cual se encarguen de investigar este tipo de hechos, los delitos informáticos son delitos en los cuales se requiere de sujetos especializados los cuales se encarguen de una investigación exhaustiva y así hallar al sujeto activo de dichos delitos y determinar su culpabilidad enmarca inminentemente en un tipo penal establecido dentro de nuestra legislación penal.

**RESUMEN ANALITICO**

En este capítulo analizamos una temática en la presente investigación la cual es muy abarcativa, por lo que se hace imposible tratarla de manera exhaustiva. El hecho de que la informática interactúa con la sociedad a velocidades exponenciales, en lugar de las lineales correspondientes a las ciencias jurídicas, nos enfrenta ante la cruda verdad de que, de no hacerse algo de manera inmediata, nos hallaremos cada día más lejos de la verdad de las conductas que pudieran resultar incriminables, en defensa de los valores reconocidos como protegibles por la sociedad que ampara al orden jurídico o que éste debe intentar salvaguardar.53

Es evidente que los principios los cuales regirían dentro el área de los delitos informáticos son el principio de legalidad y el principio de reserva penal ambos principios ayudan a una tipificación más clara y eficiente e nuevos tipos penales como es la falsificación informática, sin embargo, existe elementos como la culpabilidad, la acción u omisión la tipicidad y la culpabilidad los cuales son elementos completamente importantes para la tipificación de nuevos tipos penales dentro el área de la informática debido a que nuestra legislación penal presenta diferentes tipos de vacíos legales en los cuales se van demostrando gracias a la gran incidencia de delitos

[53]CAMPOLI, GABRIEL ANDRES. (2003). "Nuevas Tendencias Criminológicas y Victimológicas en la Sociedad de la Información", en Alfa Redi: Revista de Derecho Informático, nro. 65.

informáticos los cuales no existe una entidad ni existe la capacitación necesaria para tratar este tipo de delincuencia la cual cada día se va generando de manera rápida gracias al desarrollo de las tecnologías.

Por ello, la criminalidad informática obliga a revisar los elementos constitutivos de gran parte de los tipos penales tradicionales. Cabe imaginar el estupor de un penalista del pasado siglo XIX ante la mera alusión, hoy tan frecuente en el lenguaje, referida a la delincuencia informática, a situaciones tales como la posibilidad de que existan fraudes en los que el engaño se realiza sobre una máquina y no sobre una persona, de robos de servicio o de hurtos de tiempo en el ordenador que se realizan sin fuerza en las cosas, sin que exista un ánimo de lucro, sino un mero propósito lúdico por quien lo lleva a cabo, sin que se prive al titular de su posesión. Por tratarse de un sector sometido a constantes fluctuaciones e innovaciones tecnológicas, sus categorías son asimismo efímeras y cambiantes. Además, la criminalidad informática se caracteriza por las dificultades que entraña descubrirla, probarla y perseguirla, a ello se añade la facilidad de penetrar en los sistemas informáticos.

# ***MARCO JURÍDICO***

## CAPITULO III

## 3. MARCO JURÍDICO

### 3.1 SISTEMA PENAL EN RELACIÓN A LOS DELITOS INFORMÁTICOS Y FALSEDAD INFORMÁTICA

En Bolivia encontramos un conjunto de normas que tratan de enmarcar la convivencia social, normas que rigen el derecho familiar, derecho tributario, derecho minero derecho penal y otros, pero encontramos que existe un vacío en la normativa en cuanto al Derecho Informático y en si acerca de los delitos informáticos…"En el año 1997 bajo la batuta de Dr. Rene Blattman Bauer y con el asesoramiento del catedrático emérito de la Universidad de Basilea de Suiza el penalista alemán Gunter Stratenwer Bolivia reformo parcialmente su Código Penal introduciendo entre otras novedades los Delitos Informáticos previstos en los Artículos 363 bis y ter",(54)lo cual implicó un cambio sustancial en nuestro ordenamiento jurídico, una adecuación dictada por el orden tecnológico, estableciéndose de esta manera por primera vez en nuestra legislación, un capítulo destinado a los delitos informáticos .

La falta de tipificación de conductas delictivas en el área informática en nuestro ordenamiento jurídico penal vigente imposibilita una calificación jurídico legal que individualice a la mismas, llegando a existir una alta cifra de criminalidad e impunidad, haciéndose imposible sancionar como delitos, hechos no descriptos en la legislación penal con motivo de una extensión extralegal del ilícito penal ya que se estaría violando el principio de legalidad expreso en la máxima no existe delito si no hay ley.

[54] SAEZ Capel Jose (2014) pag 9.

Sin embargo, en nuestra actual legislación penal se encuentran tipificados tan solo tres tipos penales disponiendo lo siguiente:

**CAPITULO XI**

**DELITOS INFORMÁTICOS**

- **ARTICULO 363 bis (MANIPULACIÓN INFORMATICA)**.- El que con la intención de obtener beneficio indebido para si o para un tercero manipule un procesamiento o transferencia de datos informáticos que conduzcan a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto ocasionando de esta manera una transferencia patrimonial en prejuicio de tercero será sancionado con reclusión de uno a cinco años y con una multa de sesenta a doscientos días.
- **ARTICULO 363 ter (ALTERACIÓN ACCESO O USO INDEBIDO DE DATOS INFORMÁTICOS).-** El que sin estar autorizado se apoderare, 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 1 año o multa hasta doscientos días.

En cuanto a su contenido, ambos artículos son generales y amplios, pero no cubre, de cierta manera, la laguna legal existe, recordemos que el Código Penal señala los presupuestos para la aplicación del poder coactivo del Estado y tutela, los principios básicos de la convivencia social; si hay modificaciones en el orden social y económico, el derecho penal también deberá cambiar. En esta materia, no se admite la interpretación analógica frente a un vacío jurídico porque, de ser así, se estarían creando delitos de manera arbitraria por parte de quienes tengan a su cargo la labor de valorar el hecho. Evidentemente, tratar de encuadrar a la fuerza algunas conductas

en figuras tradicionales ya existentes sería vulnerar el principio de legalidad.

"En todo delito de los llamados informáticos, hay que distinguir el medio y el fin."(55) Para poder encuadrar una acción dolosa o imprudente dentro de este tipo de delitos, el medio por el que se cometan debe ser un elemento, bien o servicio, patrimonial del ámbito de responsabilidad informática y el fin que se persiga debe ser la producción de un beneficio al sujeto o autor del ilícito, una finalidad deseada que causa un perjuicio a otro, o a un tercero, no obstante ambos artículos están exentos a la problemática actual acerca de la delincuencia informática.

Hablando de los mismos artículos se debe citar la ineficacia de ambos ya que no siquiera tiene una pena privativa de libertad, ambos artículos determinan como sanción la prestación de trabajo de hasta de un año o multa hasta de doscientos días traduciéndose esta en una sanción insignificante, …"se considera que una pena simbólica que no posibilita que la prevención general de la norma sea efectiva en este tipo de delitos sin embargo, al respecto existe varias posturas una de las mismas señala ven el fin de la pena en la intimidación de las generalidad de los ciudadanos para que se aparten de la comisión de delitos",(56) es decir que esta privación sería una amenaza hacia la generalidad de ciudadanos respecto a una posible sanción.

Por otra parte lo más cercano a los delitos de falsificación informática dentro de nuestra legislación penal tipifica en el capítulo III los delitos de falsificación de documentos en general en dicho capítulo se tipifican una

[55] SAEZ Capel José (2014) pág. 69.

[56] MUÑOZ CONDE Francisco, (2004) pág. 48.

serie de conductas ilícitas de una manera general sin considerar de manera específica los Documentos Electrónicos, estos artículos textualmente dispone:

**ARTICULO 198.- (FALSEDAD MATERIAL**).- El que forjare en todo o en parte un documento público falso o alterare uno verdadero, de modo que pueda resultar perjuicio, incurrirá en privación de libertad de uno a seis meses.

**ARTICULO 199.- (FALSEDAD IDEOLÓGICA).-** El que insertare o hiciere insertar en un instrumento público verdadero declaraciones falsas concernientes a un hecho que el documento deba probar, de modo que pueda resultar perjuicio, será sancionado con privación de libertad de uno a seis años. En ambas falsedades, si el autor fuere un funcionario público y las cometiere en el ejercicio de sus funciones la sanción será de privación de libertad de dos a ocho años.

**ARTÍCULO 200.- (FALSIFICACIÓN DE DOCUMENTO PRIVADO).-** El que falsificare material o ideológicamente un documento privado incurrirá en privación de libertad de seis meses a dos años siempre que su uso pueda ocasionar algún perjuicio.

**ARTICULO 202.- (SUPRESIÓN O DESTRUCCIÓN DE DOCUMENTO).**- El que suprimiere, ocultare o destruyere en todo o en parte un expediente o un documento de modo de que pueda resultar prejuicio, incurrirá en la sanción del artículo 200.

**ARTÍCULO 203.- (USO DE INSTRUMENTO FALSIFICADO).-** El que a sabiendas hiciere uso de un documento falso o adulterado será sancionado como si fuere autor de la falsedad.

Frente a estas debilidades existentes en nuestra legislación penal vigente, cuando se cometen delitos informáticos en la práctica se los subsume dentro de tipos penales generales por ejemplo cuando existe falsificación informática pues se lo tipifica como uso de instrumento falsificado o bien

falsedad material o si se presenta el skimming o phishing se lo tipifica como robo etc en efecto, se demuestra la necesidad urgente de contar con una normativa jurídico penal precisa la cual sea aplicable y usada por autoridades judiciales como jueces y fiscales en la cual se tipifique nuevos tipos penales para que la misma evite problemas al momento de investigar, tipificar y sancionar conductas ilícitas con relación a una computadora u ordenador.

Por otra parte, El Convenio de Ciber delincuencia del Consejo de Europa de 23 de noviembre del 2001 llevado a cabo en Budapest define la falsificación informática de la siguiente manera:

**ARTICULO 7 .- FALSIFICACIÓN INFORMÁTICA**

- Cada parte adoptara la medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la traducción alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos con independencia de que sean legibles o inteligibles directamente las partes podrán exigir que exista una intención dolosa o delictiva similar para que se considere que existe responsabilidad penal.

Debido Al incremento de delitos informáticos en nuestra sociedad, es necesaria la tipificación de nuevos tipos penales acordes al desarrollo tecnológico con el fin de prevenir y luchar contra este tipo de delito,

**RESUMEN ANALÍTICO**

En esta parte de la presente investigación señalamos principalmente la tipificación actual acerca de los delitos informáticos en nuestro país la cual señala de manera muy general varios tipos penales, señalamos también la existencia de varias tipificaciones dentro en el área de las falsificaciones es

así que se señala la falsificación material e ideológica, sin embargo, aun así existe vacíos legales dentro del área de los delitos informáticos y las tipificaciones específicas de nuevos tipos penales es necesaria para que ayuden a combatir la ciber delincuencia.
En Bolivia los delitos informáticos son tratados como delitos comunes, están incluidos en el Código Penal y no tienen una ley específica, sin embargo, se debe actuar de forma mas eficaz para evitar este tipo de delitos debido a que actualmente se cometen con gran impunidad.

En los delitos informáticos y en si la falsificación informática, se omiten algunos detalles característicos de cada figura; por ejemplo, en el caso de acceso no se establece la diferencia entre acceso doloso y acceso culposo. Así es como se crea un universo grande para la aplicación del artículo: o todas las conductas ingresan o no hace ninguna, lo cual perjudica la labor de interpretación. Introducirnos al análisis de los delitos informáticos en su interrelación con el derecho penal implica cotejar ambos en virtud de las nuevas corrientes científica.

# ***MARCO PRACTICO***

## CAPITULO IV

## 4. FALSIFICACIÓN INFORMÁTICA

### 4.1. CONCEPTO

"Los avances de la tecnología de la información y comunicaciones y el crecimiento de la operaciones comerciales en Internet han propiciado el surgimiento de nuevas conductas fraudulentas,"(57) en si la falsificación informática es el uso, alteración modificación, creación por imitación total o parcial destrucción u ocultamiento temporal o definitivo de documento electrónicos públicos o privados por medios informáticos.

"El articulo 7 de la Convención del Consejo de Europa llevado a cabo en Budapest sobre Ciber delincuencia,"( 58 )establece la obligación de los Estados de adoptar todas las medidas, legislativas o de otra especie, para erigir en infracción penal conforme a su derecho interno, la introducción, la alteración, la eliminación y la supresión intencional y contraria a derecho de datos informáticos, la generación de datos no auténticos, con la intención de que ellos sean tenidos en cuenta o utilizados para fines legales como si fueran auténticos, sean o no directamente legibles o inteligibles. …"Además se puede exigir una intención fraudulenta o una intención delictiva similar como la requerida para la responsabilidad penal."(59)

Una convención como ésta nos propone como tarea inmediata la de estudiar hasta qué punto nuestro derecho vigente satisface las obligaciones contraídas por el Estado."Las conductas mas frecuentes relacionadas con la falsificación informática de los medios electrónicos se cometen a través del

[57]RICO Carrillo Marilina (2013) pág. 208.
[58]Convención de Ciberdelincuencia Budapest, 27 de noviembre de 2001,
[59] BACIGALUPO Zapater E. (2002) pág. 1.

uso y clonación de tarjetas magnéticas, documentos electrónicos, correos electrónicos, y páginas web."(60)La falsificación informática como objeto tendrá evidentemente el uso de las tecnologías como computadoras, medios magnéticos etc., y como instrumento tendrá documentos electrónicos, tarjetas de crédito, páginas en internet, correos electrónicos etc.

Dado el creciente número de denuncias de incidentes relacionados con la Falsificación Informática, se requieren métodos adicionales de protección. En nuestro país se esta realizando una transición en este tema ya que existe un proyecto de ley en el cual se estaría estableciendo nuevos tipos penales ampliando los tipos penales en el área informática los cuales se encuentran tipificados en nuestra actual legislación.

La falsificación informática como objeto o fin, cuando se alteran datos de los documentos almacenados en forma computarizada y; como instrumento o medio, cuando las computadoras son utilizadas para efectuar falsificaciones de documentos de uso comercial**.**

## 4.2 CLASES DE FALSIFICACIÓN INFORMÁTICA.

### 4.2.1. CONDUCTAS DE FALSIFICACIÓN INFORMÁTICA QUE TIENEN COMO OBJETO DOCUMENTOS ELECTRÓNICOS.

El delito de falsedad de documento electrónico se encuentra dentro de una serie de acciones punibles denominadas delitos informáticos pues su acción se lleva a cabo mediante un medio informático, "sin embargo la falsedad de documento electrónico tendría lugar en el supuesto de alteración de la información contenida en el documento o firma electrónica

[60]RICO Carrillo Marilina (2013) pág. 208.

circunstancia de aplicación a los cheques electrónicos o al dinero generado a través de un programa de ordenador."(61)

En el plazo aproximado de tres décadas en materia de documentos la dogmática de los delitos de falsedad documental se ha visto confrontada con diversas innovaciones tecnológicas que han obligado a reflexionar sobre la trascendencia que ellas podían tener en la aplicación de los delitos correspondientes a este ámbito. En general, informáticamente podría modificarse en parte un documento o crear un nuevo documento y hacerlo pasar por original, en si las falsificaciones informáticas están ocupando un renglón importante en el mecanismo de alteración, imitación, falsificación de documentos electrónicos.

"Los documentos electrónicos son privados por lo que la conducta de la falsificación solo se realiza en un documento privado o mercantil,"(62) es un documento cuyo soporte material es algún tipo de dispositivo electrónico o magnético, y en el que el contenido está codificado mediante algún tipo de código digital, que puede ser leído, interpretado, o reproducido, mediante el auxilio de detectores de magnetizaciones, …"es la representación en forma electrónica de hechos jurídicamente relevantes, susceptibles de ser representados en una forma humanamente comprensible."(63)

Se considera que documento es: "un instrumento, escritura, escrito con que se prueba, confirma o justifica alguna cosa que atestigüe un hecho histórico."(64)

---

[61] MORENO Navarrete M.A. (1999) pág. 149.
[62] MORENO Navarrete M.A. (1999)pág. 150.
[63] Wikipedia "documento electrónico" (en línea) es/Wikipedia.org/wiki/documento electrónico. Consulta 18/07/14.
[64] CABANELAS De Torres G pág. 134.

En este contexto se deben plantear las cuestiones referentes a la repercusión que las nuevas regulaciones tienen en el ámbito propio de los delitos de falsedad documental. Ello no es sólo consecuencia del articulo 7 de la Convención de Ciber delincuencia llevada a cabo en Budapest, cuya finalidad es indudablemente la protección penal de los documentos electrónicos, sino también de las consecuencias que esta nueva especie de documentos generan respecto del concepto de documento, especialmente en el derecho privado.

"Si bien se ve, la posibilidad de creación electrónica de documentos no ha variado el concepto de documento en sí mismo. Lo que ha cambiado son las maneras en las que se llevaban a cabo las funciones tradicionales del documento, básicamente el tipo de soporte en el cuál se perpetúala declaración de la voluntad que se documenta, la forma de garantizar el contenido de la declaración a quien la realizó y la prueba de la autenticidad mediante una certificación de determinados signos, análoga a una certificación de carácter notarial, a través de un servicio de certificación electrónico."(65)

En este contexto el incremento de las técnicas informáticas son instrumentos para cometer falsedades documentales, …"por medio de aquellas puede alterarse un documento que es registrado en el disco duro de un ordenador, en un disquete o un casete o en el CD ROM o puede introducirse un documento"(66)En ese orden de ideas, se encuentra que el mensaje de datos entendido como documento electrónico también es susceptible de ser firmado, de tener un titular o creador, e igualmente, puede diferenciarse cuando un mensaje de datos es un documento electrónico original y auténtico, en la medida que no ha sido alterado. "Por lo pronto la

[65]BACIGALUPO Zapater E. (2002) pág. 122.
[66]ORTS Enrique- Roig Margarita (2006) pág. 147

doctrina considera que el dolo eventual es suficiente respecto de la calidad de documento del objeto de la acción en los delitos de falsedad documental, lo mínimo en que un soporte electrónico puede alojar un documento a efectos penales, que exprese e incorpore datos hechos narraciones con eficacia probatorias o cualquier tipo de relevancia jurídica."(67)

Es frecuente que la misión del documento como soporte de información implique que no requiera de más valor probatorio que el que se presuma o se alegue en las menciones del documento. Por ejemplo, la fecha de publicación o el nombre del autor suelen figurar en los documentos y se suelen dar por válidos salvo prueba en contra. Sin embargo, …"en ocasiones, es preciso demostrar la autenticidad del documento electrónico o bien, algunas propiedades conexas, como la fecha de creación o publicación, el autor, el expedidor, o el titular del documento (a los efectos de atribuirle un derecho), o bien otra información registrada en sus metadatos."(68)

En este orden de cosas podemos anotar los siguientes requisitos imprescindibles para que se pueda verificar la calidad del documento electrónico:

a) Con carácter general ha de proceder de una persona determinada o determinable que actúa en nombre propio , de un tercero, de una persona jurídica de un ente publico
b) Ha de ser portador de un sentido, comprensible razonable y creíble.
c) Un sentido con algún tipo de relevancia jurídica

[67]ORTS Enrique- ROIG Margarita (2006) pág. 147
[68]Wikipedia documento electrónico [en línea] es/Wikipedia.org/wiki/documento electrónico. [Consulta 18/07/14.]

En si la falsificación del documento electrónico es la alteración, simulación o suposición de la verdad la cual se efectúa en un documento electrónico el cual es privado, tendría lugar en el supuesto de alteración de la información contenida en el documento o la firma electrónica, en este contexto la autenticidad de los documentos electrónicos se refuerza en base a un mecanismo complementario.

#### 4.2.1.1. FIRMA DIGITAL

De manera conceptual…"firma refiere que es el nombre y apellido, o título, que se pone al pie del escrito, para acreditar que procede de quien lo suscribe lo de allí manifestado para obligarse a lo declarado." (69) Por ello, la definición del diccionario requiere ser procesada pues, inclusive en el lenguaje ordinario, la firma no es la escritura del nombre y apellido o del título de una persona, sino un signo propio que permite su identificación, que jurídicamente puede ser realizada también por una persona autorizada por el titular para reproducirla en señal de reconocimiento del contenido de una declaración de algún modo documentada.

Desde el punto de vista conceptual la firma electrónica es la firma avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma, siempre que esté basada en un certificado o documento reconocido y que haya sido producida por un dispositivo seguro de creación de firma, tendrá, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel y será admisible como prueba. …"En general, la firma es el signo característico mediante el cual un sujeto expresa su reconocimiento de la declaración documentada."(70)

[69]CABANELAS De Torres G (2000) pág. 169.
[70] Wikipedia Firma Electrónica [en línea] es/Wikipedia.org/wiki/firma electrónica. [Consulta 20/08/14.]

De esta manera se puede considerar demostrado que los datos electrónicos que permiten la identificación del que reconoce una declaración determinada y documentada, no se diferencian sustancialmente con la noción de firma del lenguaje ordinario. Tradicionalmente la firma ha sido ejecutada de propia mano y constituye un signo gráfico personal difícilmente repetible por otro, pero, como se ha visto, puede ser ejecutada por otra persona y puede ser igualmente irrepetible cuando es realizada mediante datos electrónicos que sólo están a disposición del interesado. Admitida la autoría espiritual de la firma y del documento, resulta claro que la introducción de la firma electrónica en el tráfico jurídico no requiere ninguna modificación conceptual en el marco de la autenticidad del documento, auténtico será el documento cuando el uso del conjunto de los datos informáticos que se utilizan como medio para identificar al autor de la declaración haya sido puesto por una persona autorizada y no provenga de un abuso del secreto de las claves que lo garantizan. Por lo tanto, la firma electrónica y el documento electrónico requieren siempre un certificado reconocido, es decir una certificación de la firma puesta en el documento por un prestador de servicios de certificación que tiene lugar por medio de componentes técnicos que constituyen un determinado software o hardware.

Para resumirlo de forma sencilla, la firma electrónica es un conjunto de datos que nos permiten acreditarnos y cerrar acuerdos por medios electrónicos, principalmente por Internet, la certificación…"es una comprobación que se producirá por regla en forma totalmente automática y a través de un aparato técnico de creación humana que actúa por sí mismo. Si esto se trata de un tipo penal exteriormente análogo o paralelo al tipo del delito de falsedad documental, que, sin embargo, no protege documentos sino evidencias sensibles con efectos probatorios."(71)

[71]BACIGALUPO Zapater Enrique. (2002) pág. 123.

### 4.2.2. CONDUCTAS DE FALSIFICACIÓN INFORMÁTICA QUE TIENEN COMO OBJETO EL INSTRUMENTO DE PAGO

"El desarrollo de los instrumentos electrónicos de pago junto con el avance de la informática han propiciado el surgimiento de nuevas conductas delictivas a la vez generan ciertos patrones los cuales dificultan el encuadramiento en los tipos penales tradicionales."(72). Definimos a la tarjeta magnética…"como el documento emitido por una entidad generalmente un banco mediante el cual una persona el titular, puede obtener una serie de prestaciones."(73)Con la modernidad se va dando una relación entre la entidad que emite las tarjetas magnéticas y el titular de la tarjeta y generan una relación comercial ya que mediante la tarjeta magnética se puede realizar desde pagos de servicios hasta cobros de dinero esta situación se ve en la cotidianidad de las personas.

Entre las conductas más frecuentes que tienen como objeto el medio de pago encontramos a la clonación de tarjetas y la falsificación el apoderamiento indebido de datos, estas conductas conducen a la ilícita del instrumento de pago se traduce en la disposición indebida del dinero o del crédito asociado con el correspondiente perjuicio económico para el titular legítimo de la cuenta bancaria que es el único autorizado para la utilización del instrumento de pago tal es el caso por ejemplo la utilización de cajeros automáticos en los cuales los delincuentes informáticos introducen un lector de chip en el cual copian la información personal de cada tarjeta magnética solo para llegar a clonar dicha información y haber retiros de dinero sin embargo, estas situaciones de cierta manera se deben a la inseguridad jurídica existente en Bolivia por la ya mencionada ausencia de legislación la cual ofrezca seguridad y protección a los usuarios.

[72]RICO Carrillo Marilina (2013) pág. 211.
[73] SAEZ Capel José. (2014) pág. 205.

### 4.2.2.1. CLONACIÓN.

"En los últimos años ha aparecido un supuesto delictivo conocido comúnmente como clonación de tarjetas el termino clonar actualmente se usa para designar el fenómeno de la reproducción fraudulenta de tarjetas de pago que se lleva a cabo a través de la duplicación de los datos normalmente contenidos en la banda magnética del instrumento original."(74)

"Sin embargo los casos más comunes de clonación son en los comercios tradicionales y en cajeros automáticos y se lleva a cabo mediante el uso de un dispositivo conocido como skimer que permite copiar los datos de la banda magnética de la tarjeta una vez los datos copiados son procesados a través de un equipo informático y un software que capta la información y permite incorporarla a una tarjeta nueva creando de esta manera la duplicación de la tarjeta original. La utilización de este dispositivo ha generalizado el uso del término skimming como omnicomprensivo de las situaciones donde se produce el robo de la información de las tarjetas como consecuencia de una utilización legitima del instrumento de pago."(75)

Concretamente se denomina skimming al robo fraudulento y con fines delictivos de la información contenida en las tarjetas bancarias de crédito o débito y esta información está compuesta por datos personales y secretos del usuario de la tarjeta y son usados identificados e individualizados por la red informática bancaria, el fin de este robo es permitir a los delincuentes clonar la información y posterior uso de la misma, los lugares más comunes del skimming es en gasolineras, restaurantes y bares al momento de pagar o bien en el momento de usar un cajero electrónico, esta actividad se realiza mediante un lector de tarjetas portátil oculto sin embargo, esta actividad se realiza debido a la inseguridad jurídica existente en Bolivia por la ya

[74] RICO Carrillo Marilina. (2013) pág. 212
[75] RIOS Carrillo Marilina. (2013) pág. 212

mencionada ausencia de legislación la cual ofrezca protección respecto a los delitos informáticos.

#### 4.2.2.2. FALSIFICACIÓN

En el ámbito de las tarjetas de crédito la falsificación puede darse como consecuencia de la clonación, sin embargo, también puede darse como supuesto de elaboración de tarjetas falsificadas independientemente de un proceso de clonación donde la conducta se limita a la fabricación de un nuevo instrumento de pago mediante la copia de los datos del instrumento original, "en la mayoría de estos casos se da en consecuencia a un ataque informático a las empresas propietarias de las tarjetas las cuales mantienen bases de datos con la información de estos medios de pago."(76)

"La falsificación de instrumentos electrónicos de pago, donde se incluyen los cheques electrónicos y el dinero efectivo electrónico, también tiene lugar cuando se produce una alteración en los datos originalmente incorporados en los documentos representativos de estos medios de pago."(77)

### 4.2.3. CONDUCTAS DE FALSIFICACIÓN INFORMÁTICA QUE TIENEN COMO OBJETO PAGINAS DE INTERNET Y USO DE CORREOS ELECTRÓNICOS.

"La captación de datos es una práctica que facilita la comisión de delitos de falsificación informática en el cual se perpetra a través del uso de esos datos con fines fraudulentos."(78) El apoderamiento indebido de los datos también es una consecuencia de la falsificación informática, gracias al desarrollo sofisticado de prácticas de captación y apoderamiento de datos.

[76] RICO Carrillo Marilina. (2013) pág. 213
[77] RICO Carrillo Marilina. (2013) pág. 213
[78] RICO Carrillo Marilina. (2013) pág. 213.

Dentro de la figura de la falsificación informática existen dos figuras de captación y apoderamiento ilícita de datos a través del Internet que serían el phishing y el pharming.

#### 4.2.3.1. PHISHING

En si el phishing se denomina a toda clonación de páginas webs a acción de liberada de crear una copia idéntica de una determinada página web es un método que usan los cibercriminales para engañar a los usuarios y tener acceso a datos personales del usuario generalmente este delitos es cometido a través de la clonación de paginas webs de instituciones bancarias de las cuales son sustraídos datos personales de los usuarios de dicha institución con fines ilícitos . “En el phishing la captación ilícita de datos tiene lugar a través del envió masivo de correos electrónicos que simulan la identidad de una institución financiera con el objetivo de solicitar a los receptores los datos de sus respectivas tarjetas alegando diferentes motivos.”(79)

Phishing o suplantación de identidad, es un término informático que denomina un tipo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria. …”El término phishing proviene de la palabra inglesa fishing, haciendo alusión al intento de hacer que los usuarios muerdan el anzuelo. Los pescadores de clientes ingenuos de la banca para acceder a su contraseñas secretas y robar sus ahorros circulan por los correos electrónicos de la población, hay pruebas de clonación de dos paginas web de bancos locales que buscaban estafar a los usuarios. La prevención es la única salida en un

[79] RICO Carrillo Marilina . (2013) pag 214

mundo donde los engaños informáticos se tornan cada vez mas sofisticados y en Bolivia no es la excepción."(80)

Dado el creciente número de denuncias de incidentes relacionados con el phishing en Bolivia desde la gestión 2006, se requieren métodos adicionales de protección en contra de esta forma de falsificación informática que es el phishing. Se comete el phishing, ya sea el envío global de millones de correos electrónicos bajo la apariencia de entidades bancarias, solicitando las claves de la cuenta bancaria o con ataques específicos.

"El phishing se da por ejemplo Un usuario al que se le contacta mediante un mensaje electrónico y se le hace mención sobre la necesidad de verificar una cuenta electrónica puede o bien contactar con la compañía que supuestamente le envía el mensaje, o puede escribir la dirección web de un sitio web seguro en la barra de direcciones de su navegador para evitar usar el enlace que aparece en el mensaje sospechoso de phishing."(81)

### 4.2.3.2. PHARMING

"En el pharming también remite a los usuarios a páginas web falsas creadas en formato similar a las de las identidades bancarias con el objeto de captar los datos de los clientes, evidentemente vulnerando el nombre de sistema de dominio permitiendo al atacante redirigir el nombre de dominio de la identidad a una pagina web que en apariencia es idéntica."(82)

Pharming es la explotación de una vulnerabilidad en el software de los servidores del sistema de nombres de dominio o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio a otra máquina distinta. De esta forma, un usuario que introduzca un

[80] . BALBOA Gómez M. (2007)pag 10.

[81] Wikipedia Pharming[ enlínea] es/Wikipedia.org/wiki/pharming. [Consulta 14/07/14.]

[82] RICO Carrillo M. (2013) pág. 214.

determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio. La palabra pharming deriva del término farmy está relacionada con el término phishing, utilizado para nombrar la técnica de ingeniería social que, mediante suplantación de correos electrónicos o páginas web, intenta obtener información confidencial de los usuarios, desde números de tarjetas de crédito hasta contraseñas. El origen de la palabra se halla en que una vez que el atacante ha conseguido acceso al sistema de nombres de dominio.“Todos los ordenadores conectados a internet tienen una dirección IP única. Estas direcciones IP son comparables a las direcciones postales de las casas, o al número de los teléfonos, debido a la dificultad que supondría para los usuarios tener que recordar esas direcciones IP, surgieron los Nombres de Dominio, que van asociados a las direcciones IP del mismo modo que los nombres de las personas van asociados a sus números de teléfono en una guía telefónica.”(83)

La técnica de pharming se utiliza normalmente para realizar ataques de phishing, redirigiendo el nombre de dominio de una entidad de confianza a una página web, en apariencia idéntica, pero que en realidad ha sido creada por el atacante para obtener los datos privados del usuario, generalmente datos bancarios.…“Para verificar si la página es verdadera y no es una página falsa, la clave está en mirar de arriba hacia abajo la página virtual es decir se debe verificar si el nombre de dominio escrito en la parte superior del navegador coincide con la dirección que sale en la parte inferior izquierda de la pantalla.”(84)

Para evitar ser víctima de estos delitos deberá tomar en cuenta las siguientes recomendaciones:

[83] Wikipedia Phishing [en línea] es/Wikipedia.org/wiki/phishing. [Consulta 14/07/14.]
[84]BALBOA Gomez M. (2007)pag 10.

a) Ignorar los mensajes de correo electrónico no solicitados que piden acceder a estos sitios web que exijan información de cuentas, números de tarjetas, pines o claves no usar estos enlaces para acceder a sitios webs sensibles como la banca electrónica.
b) Asegurarse de que el sitio al que le solicitan el ingreso sea realmente un sitio seguro y perteneciente a la empresa.
c) Si tienen contacto conocido con la institución solicite telefónicamente su dirección de correo para que le ratifiquen el enlace a su página web ya que este tipo de ataques simulan hasta el más mínimo detalle de la página web.
d) Por ningún motivo entregue información acerca de su número de tarjeta pin pasword o número de cuenta que así lo soliciten esa información debe ser solo de su conocimiento.
e) No se suscriba a ninguna lista o página desconocida o sitio que no cuente con un verificativo de seguridad autorizado.(85)

En ambos casos el modus operandi exige la elaboración de una página web falsa cuya acción capta datos personales de tal forma en la que se apodera de dicha información para fines ilícitos contando de manera exacta con los datos personales de los usuarios.

## 4.3. EL BIEN JURÍDICO TUTELADO POR EL TIPO PENAL DE LA FALSIFICACIÓN INFORMÁTICA

Este instituto se puede analizar desde dos perspectivas, ya sea a través de quien lo detenta como un derecho o bien para quienes resulta un precepto, ya que es un mecanismo jurídico estructurado y su existencia es en función de proteger un bien jurídico. Por excelencia, la información, se perfila como la esencia de este instituto, sin embargo, debemos tener en consideración

[85]BALBOA Gomez M. (2007) Pág. 10.

que existen otros intereses que se protegen. Se está protegiendo esencialmente la información pero, al ser los delitos informáticos pluriofensivos, accesoriamente se resguardan la fe pública, la propiedad, la seguridad del Estado y, finalmente, se protege la intimidad del usuario o titular de la información, amparándolo de posibles daños o perjuicios. Ahora bien, puesto que el Derecho Penal debe tomar en cuenta las garantías individuales y que el manejo inadecuado de la información genera responsabilidad criminal, son necesarias normas especiales que operen en defensa de las garantías conculcadas.

La importancia de la información y de su protección en la sociedad actual se refleja en los siguientes ejemplos: en el campo mercantil, los actos de comercio que se realizan a través de la red o utilizando bases de datos para almacenar sus recursos, es el denominado comercio electrónico; con respecto a las relacione empresa - cliente, aparecen formas alternativas de hacer comercio como en el caso de acceder a la página principal de repuestos de autos y poder hacer el pedido directamente, pagando con el número de su tarjeta de crédito o en del manejo de fax y del correo electrónico, para obtener cotizaciones, comprar, pagar, vender.

En general, estamos desprotegidos ante esta nueva ola de delitos. Se requieren legisladores visionarios para elaborar una legislación completa que los prevenga detalladamente, que este orientada desde una perspectiva penal, a partir de los tres rasgos fundamentales del sistema informático: la integridad, la confidencialidad y la disponibilidad de información.

### 4.4. EL ÓRGANO JUDICIAL BOLIVIANO ANTE ESTA PROBLEMÁTICA

Este tipo de delitos por su naturaleza trasnacional, suelen ser cometidos a distancia fácilmente cruzan las fronteras de los países; lo que genera unas serie de problemas de jurisdicción al no contar nuestro país con unas

legislación acorde con el derecho internacional que tipifique este tipo de delitos se genera un problema que se refleja en dos aspectos:

- El primero es que imposibilita su prosecución mas alla de las fronteras
- El segundo relacionado con la jurisdicción imposibilita que otros países puedan perseguir a los sujeto que incurran con estos delitos siendo asi que nuestro país se convertiría en una especie de refugio para los delincuentes informáticos

Por otra parte, en el caso de haberse dado una conducta nociva como la falsificación informática relacionada con el uso del ordenador, el juez esta forzado a declarar la impunidad del hecho o encajar la acción en algún tipo penal convencional, como: el fraude informático como hurto, estafa, la falsificación informática como falsedad material o ideológica, el sabotaje informático como delito de daños y estragos.

En franca violación del principio de legalidad y del deber de no usar la analogía para la interpretación de la norma penal. En la ausencia de estos elementos el juez fallaría sobreseyendo la causa por no considerar la conducta un delito. El nuevo modus operandi acerca de la falsificación informática revela situaciones que escapan al derecho penal tradicional y quedan sin protección los contenidos inmateriales del sistema informático, su integridad, su disposición o su exclusividad, estos hechos propugnan la promulgación de normas específicas. Entre los problemas más comunes para los jueces están: la violación a la privacidad; falsificación de documentos de pago; falsificación de documentos electrónicos; falsificación de páginas electrónicas; los crímenes económicos.

La dificultad probatoria que existe respecto a la falsificación informática que por su naturaleza dejan rastros muy escasos, para tal efecto se ve la

necesidad de capacitar a los operadores de justicia e investigadores de la Policía Nacional.

### 4.5. EFECTOS NEGATIVOS DE UNA REGULACIÓN IMPRECISA

Entre las desventajas podemos citar la pérdida de prestigio para el país, ya que desmejora la imagen de un mercado atractivo para las inversiones; originando una situación de marginación del orden internacional. Por otro lado, esta ausencia de figuras concretas daría lugar a la impunidad de los autores o a la forzada aplicación de preceptos que no se ajusten a la conducta. Pese a ello, no es suficiente una adecuada legislación; la misma debe ir acompañada de un programa de difusión sobre las posibles conductas ilícitas y la manera de prevenirlas. Es importante destacar que sino existe concientización acerca del riesgo que corremos, el usuario estará sometido a amenazas indiscriminadas y en varios casos ser victimas de la falsificación informática, muchas personas se preguntarán qué peligro puede derivarse de que alguien lea la información de otro. No hay que olvidarse que la informática pone en juego la intimidad de la persona, su identidad, su libertad y su intimidad, derechos que deben ser respetados por toda la comunidad incluidas las autoridades; la excepción se da cuando en bien común está comprometido. Una vez expuestos los puntos de convergencia o generadores de vacío en nuestro ordenamiento legal, cabe señalar cuáles son los problemas y qué solución debe proporcionarse. Ha quedado demostrado el problema de la adecuación típica y la vulneración al principio de legalidad por el mal uso de analogías. Por tanto, es necesario tomar medidas al respecto.

Al utilizar tipos penales a la hora de tipificar una conducta delictiva en la cual se han utilizado para delinquir como medio u objeto la tectologías de la información y comunicación, genera una evidente dificultad para los operadores de justicia, al momento de realizar una eficaz investigación y

posterior procesamiento penal, esto debido al principio de legalidad consagrado en nuestras actual Constitución política de el Estado y Código Penal vigentes en la actualidad en nuestro país, a esto se le suma la imposibilidad que genera esta falta de tipificación especial de poder perseguir a estos delincuentes más allá de nuestras fronteras.

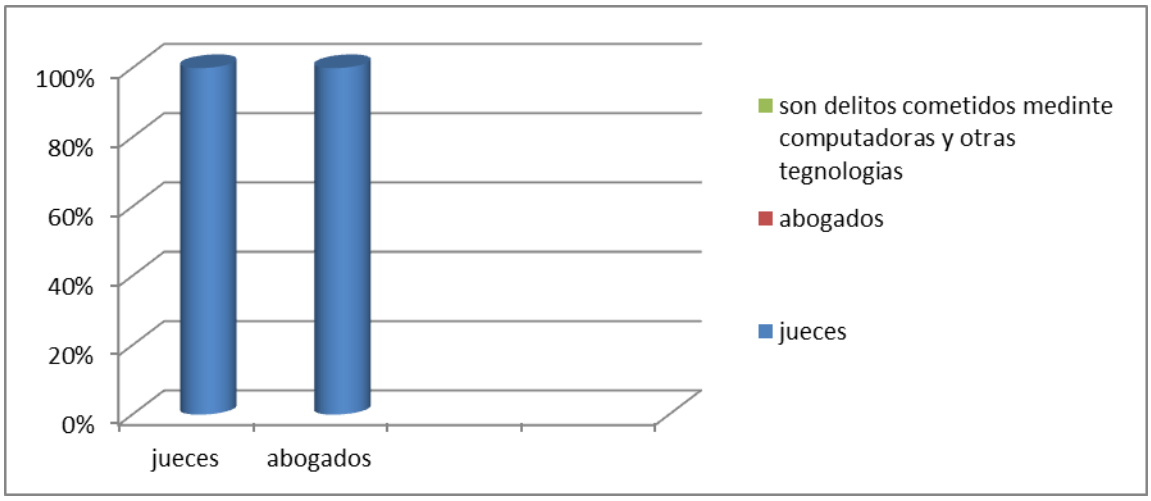
## 4.6. ANÁLISIS DEL PAPEL DEL FALSIFICACIÓN INFORMÁTICA EN BOLIVIA

Dado que no existe un estudio específico del papel de la Falsificación Informática en Bolivia se procedió a realizar entrevistas a dos grupos poblacionales, en las cuales tienen importancia sobre todo cualitativa: por un lado a profesionales abogados y por otro lado a jueces del área penal, con el fin de establecer principalmente cual es el papel dentro del sistema penal de la Falsificación Informática y para analizar la posibilidad de su incorporación en nuestra actual Normativa Penal. Aquí solamente se presentarán los resultados sobre las respuestas de la Falsificación Informática como delito informático.

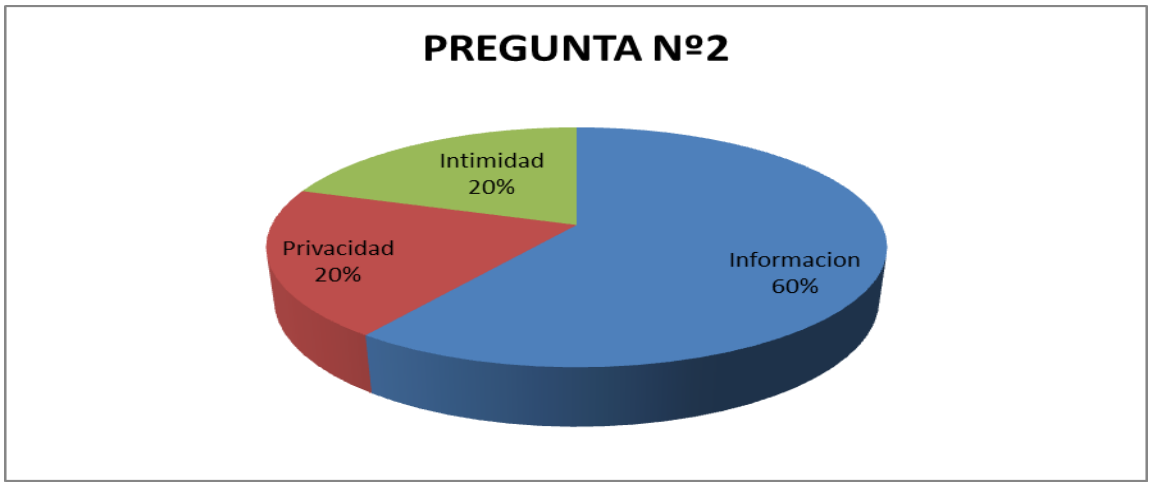
Se realizaron 50 entrevistas a profesionales abogado, y 20 a jueces del área penal, cuyo cuestionario se acompaña en el ANEXO B, de las cuales se tienen las siguientes conclusiones:

En las entrevistas a profesionales abogados del total el 100% señalaron que los delitos informáticos son aquellas conductas criminales los cuales están involucrados con una computadora.

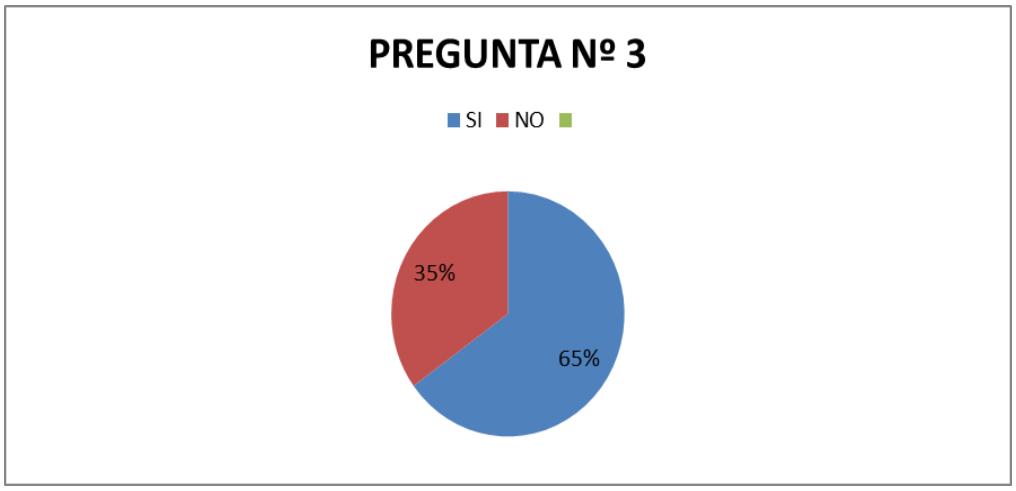
Mientras que las entrevistas a las autoridades de Órgano Judicial el 100% señalaron que los delitos informáticos son todas aquellas conductas criminales mediante el uso de las computadoras y de las tecnologías.




Respecto a que afecta los Delitos informáticos todas las personas entrevistadas coincidieron que los delitos informáticos afectan generalmente a la información, privacidad e intimidad de las personas.




En las entrevistas a los funcionarios del Órgano Judicial y abogados el 65% señalaron que la falsificación informática en Bolivia, debería ser tomada en cuenta como nuevo tipo penal ya que en legislaciones de otros países ya estaría inserta dentro de su legislación Penal 35% señalaron que este nuevo tipo penal es necesario sin embargo también hicieron notar que es necesario la incorporación de nuevos tipos penales acerca de delitos informáticos para que no exista mas vacíos legales en el área informática.




Respecto a los aspectos positivos de la incorporación de la Falsificación informática en nuestra actual Legislación Penal todos los entrevistados coincidieron que el efecto positivo es que se evitara mayor daño a la información intimidad y privacidad de las personas.

Respecto a la relación entre la existencia de viabilidad de la Incorporación de la falsificación informática en nuestra actual Legislación Penal se tienen las siguientes conclusiones:

- En el total de las entrevistas, a abogados y funcionarios del Órgano Judicial coincidieron que es viable y factible la Incorporación de la falsificación informática en el Sistema Penal Boliviano ya que en el área de delitos informáticos de Nuestro Código Penal hace falta la incorporación de nuevos tipos penales.

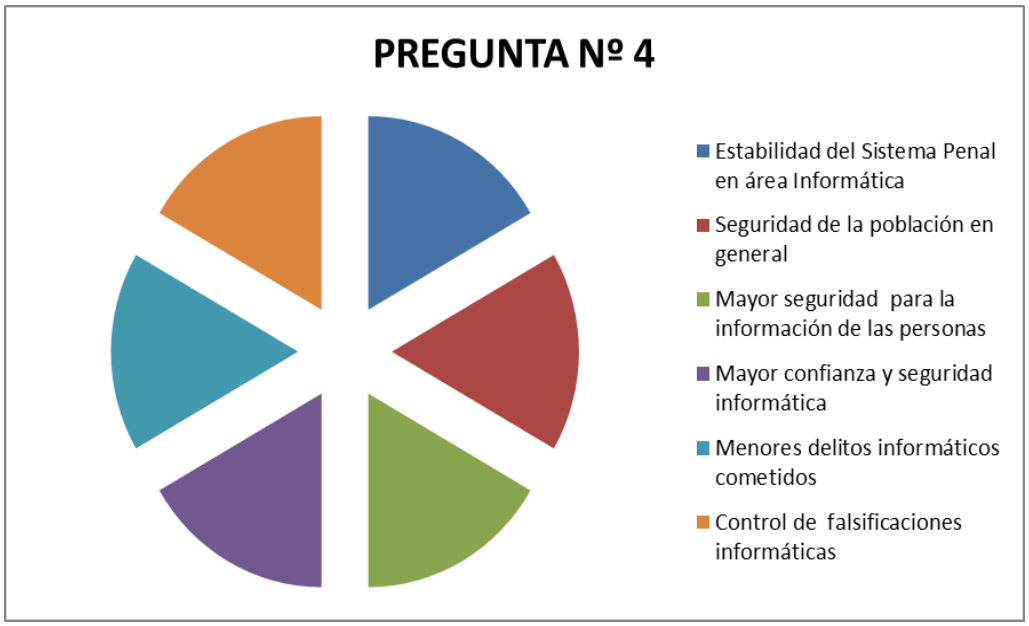
Entre las entrevistas a profesionales abogados del total el 90% señalaron que están de acuerdo con la incorporación del Nuevo Tipo Penal de la Falsificación informática mientras el 10% señalaron que no están de acuerdo.

Los argumentos a favor de la Incorporación de la falsificación informática dentro de nuestra actual legislación Penal son principalmente referidos a que muchas empresas y personas utilizan este nuevo delito para conseguir información o datos de las personas para beneficio del sujeto activo.

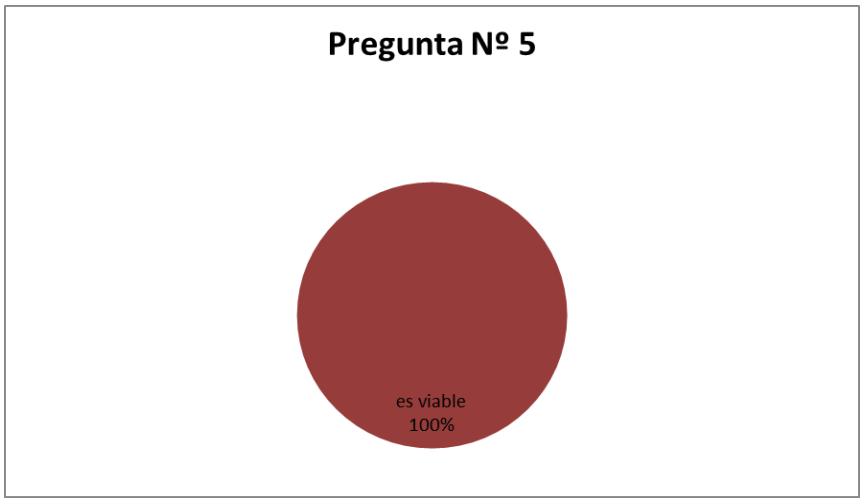
Entre las entrevistas a Jueces del área penal el 100% señalaron que es necesario determinar un la falsificación informática como nuevo tipo Penal debido a la alta incidencia de este nuevo delito informático y que se tendría que incorporar nuevos tipos penales en nuestra actual legislación penal para que no exista lagunas jurídicas.

Como efectos positivos de la Incorporación de la Falsificación Informática en el Código Penal se han señalado de las entrevistas se puede determinar lo siguiente:

- ✓ Estabilidad del Sistema Penal en área Informática
- ✓ Seguridad de la población en general
- ✓ Mayor seguridad para la información de las personas
- ✓ Mayor confianza y seguridad informática.
- ✓ Menores delitos informáticos cometidos
- ✓ Control de falsificaciones informáticas




A la pregunta sobre la viabilidad de la incorporación de la falsificación informática señalaron, en general más el 100% que es viable y entre las justificaciones para su respuesta predomina que los artículos acerca de los delitos informáticos en nuestra actual legislación penal tiene muchas lagunas legales y que por lo general no tiene una interpretación exacta y que es muy general y que la incorporación del tipo penal de la falsificación informática es necesaria ya que la tecnología esta en constante desarrollo y se van dando nuevos crímenes relacionados con la Informática.




Por tanto y en general, se puede concluir que de acuerdo a la percepción de los funcionarios de Órgano Judicial, y profesionales abogados la necesidad de incorporar en Nuestro actual Código Penal el tipo penal de falsificación informática es viable y que su establecimiento ayudaría con el desarrollo y desenvolvimiento del sistema penal en el área Informática debido a que la tecnología se encuentra en constante desarrollo.

## 4.7 EXPERIENCIAS NACIONALES E INTERNACIONALES EN RELACIÓN A LA FALSIFICACIÓN INFORMÁTICA.

Un caso de Falsificación en nuestro país por aproximadamente 500.000 dólares es investigado por la Policía desde el 22 de marzo de 2014. La jefa de plataforma de la entidad afectada, Ana María C. C., es buscada y sindicada de estafa y manipulación informática. De acuerdo con el cuaderno de investigaciones, el pasado 21 de marzo, la cliente Elsa T. P. presentó un reclamo por el débito de más de 110.000 dólares de su cuenta de ahorro sin su autorización ni firma. Denuncia que fue verificada y constatada por la casa matriz de la entidad financiera con sede en Santa Cruz. Después de una auditoría interna, la Gerencia del Banco Ganadero identificó a la presunta responsable del desvío de fondos de ésa y otras cuentas cuyos titulares desconocían esos movimientos. Las transferencias fueron

efectuadas entre febrero y marzo de 2011. De acuerdo con los comprobantes de débito, a los que La Prensa tuvo acceso exclusivo, se evidenció que la funcionaria realizó cuatro traspasos de cuenta por 91.318 dólares de una; $us 3.099, de otra, y 5.315 de una tercera, el 10 febrero; y 9.415 dólares el 11 de febrero. Posteriormente, estas sumas fueron retiradas con firmas y cédulas de identidad falsas en complicidad con otro funcionario, cajero, que fue citado a declarar ante la Fiscalía y actualmente es investigado. La gerencia del Banco Ganadero de La Paz descubrió, a través de una investigación interna hecha con cámaras de seguridad, que fue la misma funcionaria quien realizó los desvíos y retiros de dinero de las ventanillas de la entidad. Por ese motivo, esa casa bancaria presentó una denuncia en contra de la sindicada por los delitos de estafa, manipulación informática, hurto, falsificación de documento privado y uso de instrumento falsificado, que se procesa actualmente. Un investigador de la FELCC comentó que el banco no fue intervenido aún por el ente regulador del Estado. Se presume que el monto del fraude económico es superior a los 500.000 dólares. Sin embargo gracias ala investigación realizada la denunciante señalo que a su correo electrónico le llego un mensaje del Banco Ganadero el cual solicitaba la información de contraseña de la cuenta en la cual se encontraba el dinero, la denunciante sin dudarlo envió los datos de su contraseña, de esa manera la ex funcionaria del Banco Ganadero Obtuvo los datos e la cuenta y logro hacer los retiros mencionados Entretanto, voceros de la Autoridad de Fiscalización del Sistema Financiero (ASFI) afirmaron desconocer la existencia de un falsificación o estafa en el Banco Ganadero de La Paz."(86)

Aproximadamente hace un año el portal del Ministerio de Trabajo fue hackeado por personas aun no identificados en la cual se publicaba una base de datos de la instituciones en la cual revelaba nombres y paswords de varios funcionarios de esta institución, de la misma forma hackeron la

[86] PHISHING [en linea] http://www.enlacesbolivia.net/sp/noticias_proc.asp?Seleccion=471#sthash [Consulta 24/11/14]

cuanta del sistema de la Policía Nacional Boliviana en la cual consiguieron nombres de usuarios y paswords de oficiales, clases y funcionarios de dicha institución procediendo de la misma forma a publicar estos datos lo cuales son completamente confidenciales, de la misma forma hubo un ataque a la empresa nacional Entela en la cual revelaron cuentas, e-mails de usuarios de dicha empresa telefónica que permitían a cualquier persona acceder modificar, enviar y eliminar mensajes de manera sencilla de las cuentas personales y confidenciales de los usuarios.

“Un total de 15.661 tarjetas de crédito y 409.325 tarjetas de debito deberán ser sustituidas por el nuevo sistema que cuenta con chips de seguridad, por las entidades de intermediación financiera en Cochabamba, hasta diciembre de 2013, informó la Autoridad de Supervisión del Sistema Financiero (ASFI).La entidad explicó que la tarjeta registra en el chip datos de las transacciones del usuario que son únicos y que hacen imposible su clonación.

A la fecha, el sistema financiero nacional reporta más de 91 mil tarjetas de crédito y las de débito suman casi 2,3 millones de unidades. Esta entidad aseguró que el cambio se realiza para garantizar la seguridad de las tarjetas bancarias y sobre todo para eliminar las posibilidades de clonación, que ha provocado graves conflictos a usuarios de estos servicios en todo el mundo. En la explicación vertida desde la ASFI, las nuevas tarjetas con chip están vinculadas a la aplicación del estándar de operatividad EMV (Europa, MasterCard, VISA) para la autentificación de pagos mediante tarjetas de crédito y débito. Según la explicación vertida, las tarjetas chip permiten que los datos personales sólo sean accesibles a sus titulares. Esto es posible gracias a que llevan inserta una memoria que almacena las transacciones realizadas, siendo las mismas corroboradas al momento de ser utilizada nuevamente, de esta manera, por más que se logrará clonar la tarjeta se

requeriría también que las transacciones registradas en el chip de la tarjeta clonada sean coincidentes con la original, lo cual es muy difícil. Es por este motivo que las tarjetas con chip prácticamente no se pueden clonar.

Sin embargo, en la ciudad de La Paz se realizó la clonación de tarjetas de débito y crédito pertenecientes al Banco Unión, existe actualmente dos personas extranjeras de nacionalidad colombiana detenidas preventivamente, la forma de operar sostiene el fiscal asignado al caso, es mediante la clonación de chip el cual se encuentra en cada tarjeta de debito o crédito la cual contiene información personal del usuario asi como los datos de la cuenta.

“Estos dos últimos meses se incremento masivamente la ola de phishing en nuestro país, el tema de aguinaldos y mayor movimiento económico llama la atención de estos delincuentes mal llamados hackers, que no son otra cosa mas que delincuentes comunes. Recientemente se vieron traficando por internet una serie de correos phishing dirigido a los clientes de varios Bancos del sistema financiero boliviano. Algunas entidades ya efectuaron su denuncia ante la FELCC para determinados casos y se encuentran tomando medidas de seguridad técnico informáticas así como operativas para prevenir este tipo de fraudes. Sin embargo no se tiene todavía un camino claro para combatir de manera continua las amenazas actuales y las que se vienen.”(87)

Los Bancos que cuentan con soluciones de doble factor de autenticación para sus transacciones electrónicas fueron escasamente afectados por ataques de phishing, sin duda minimiza en gran porcentaje el fraude

[87]Wikipedia “phishing” ( en línea) es/Wikipedia.org/wiki/phishing. [Consulta 18/07/14].

informático y personalmente considero la mejor forma para protegerse contra el phishing.

Las medidas que ayudan pero no son suficientes para contrarrestar el phishing son las operativas, ejemplo: limitar montos de dinero para transferencias, limitar cantidad de transferencias y traspasos, enviar correo de confirmación de la operación, alertas de movimientos inusuales, el phishing no es mas que una falsificación solo que ahora se lo realiza a través de computador, no es un ataque sofisticado, ni si quiera el pharming que viene a ser la evolución del phishingse podría considerar un ataque sofisticado y mucho menos avanzado, ya que también lo realizan muchachos de entre 17 y 20 años en nuestras Universidades, en menos de 5 minutos programan un script tipo troyano que modifica el fichero host de Windows y lo wrappean en cualquier programa, diseñar una plantilla de autenticación similar al del banco y sobreponerla al original les lleva otros 5 minutos.

Los Bancos están buscando contramedidas técnicamente sofisticadas para un ataque que no es sofisticado, no digo q estas contramedidas sean malas, pero tampoco están bien dirigidas para el phishing en particular. Hay q tomar en cuenta que no están atacando nuestras redes ni aplicaciones, están atacando la ingenuidad, inocencia y buena fe de las personas. Por tanto hay q combatir nutriendo a las personas de información precisa…"En una era tecnológica, las personas no pueden quedar al margen de los cuidados mínimos en transferencias electrónicas, por más q cueste esfuerzos y dinero, se debe insistir en estas campañas de concientización y los bancos si bien no tienen la culpa, tienen la responsabilidad de su difusión."(88)

[88] PHISHING [en linea] http://www.enlacesbolivia.net/sp/noticias_proc.asp?Seleccion=471#sthash [consulta 24/11/14.]

“Cuando César Alexis Atoche Paredes hackeó la página web de la Oficina Nacional de Emergencias del Ministerio del Interior de Chile, en 2008, y escribió: El pisco es peruano, dejó entrever su baja estafa y falsificación. Un año después se convirtió en un avezado delincuente que clonaba portales de bancos de varios países para robarles a los clientes. Por ese delito lo capturaron, pero fue puesto en libertad condicional y siguió con sus fechorías.

Normalmente, los ataques se producen desde países cuyo idioma no es el Español, por ende se encontraran muchos errores en el mensaje de correo electrónico, como es este el caso, pues mezclan palabras en inglés y español. De igual forma existen muchos errores de ortografía. Sí, por curiosidad accedemos al link enviado en el correo electrónicos, digitemos un número de cuenta falso, al igual que un password falso, si la página inmediatamente nos arroja un error de clave o número de tarjeta invalido, la página puede ser real. Si por el contrario accede pero solicita la segunda clave o coordenadas de firma del cliente inmediatamente después, estamos ante una página falsa. Los bancos no requiere la segunda clave a menos que se vaya a realizar transferencias a otras cuentas. Por ello los atacantes requieren la segunda clave o coordenadas. Por último, pero no menos importante: Los bancos o entidades financieras no solicitan a sus usuarios la actualización de su información amenazando con cerrar o bloquear la cuenta.

Cada vez se registran menos asaltos a mano armada en los bancos, pero no es porque los delincuentes se hayan vuelto más honestos. Es porque ahora existen nuevos métodos para robar a entidades financieras. Principalmente tres, conocidos como pharming, phishing y malware. Los colombianos perdieron US$ 40 millones ($79 billones) el año pasado por cuenta del fraude financiero, según David Castañeda, director de investigación y desarrollo de

EasySolutions. En total, casi 10 millones de usuarios colombianos fueron víctimas de algún tipo de fraude en las plataformas virtuales.

El phishing o suplantación de identidad es el más usado, con 60% de los casos; le sigue el pharming o suplantación web, 25%, y el malware (código malicioso), con 15% de ejecución en los entornos digitales y plataformas online.

Los bancos latinoamericanos han empezado a diseñar estrategias para solucionar este tipo de delitos, que ahuyentan a los usuarios. Según el estudio Visión de Consumidores Latinoamericanos 53% de quienes no utilizan internet para transacciones bancarias o pagos tienen como razón principal el miedo al fraude. 40% de los encuestados no recuerda ninguna campaña que su banco haya realizado acerca del fraude electrónico. Prueba de que el conocimiento sobre amenazas electrónicas todavía es muy bajo.

“Pharming es una sustitución exacta de los sitios web bancarios, sus gráficos, colores y el total de sus características, para confundir al usuario a la hora de entrar a la plataforma y puedan serle hurtados los datos financieros. Entre los bancos internacionales que más prevenciones toman frente a este fenómeno están el Banco Ganadero Bolivia, el National Bank of Dominica, el Geauga Savings Bank, entre otros. Notamos un incremento cercano a 50% en los incidentes de phishing, pharming y malware en el mundo, una peligrosa realidad que afecta a la banca colombiana. Manuel Escobar, un empleado bancario de Bogotá, dice que todo se veía totalmente legal. Hasta que se dio cuenta que no era sí. Pero ya era demasiado tarde. La pérdida era total. Lo único que sé es que recibí un correo, que sinceramente parecía totalmente hecho por el banco, diciéndome que debía cambiar mi contraseña por cuestiones de seguridad. Pero cuando luego fui al banco a retirar un dinero que necesitaba, la cuenta estaba vacía. Cuando me

di cuenta era muy tarde y había perdido todos mis ahorros, relata Escobar. El phishing ocasiona pérdidas anuales por unos US$ 93 mil millones de dólares, y afecta a unos 2.500 bancos que operan en la región, de acuerdo a un estudio reciente sobre ciber crímenes hecho por el Registro de Direcciones de Internet para América Latina y Caribe."(89)

Brasil es el principal destino de los atacantes debido a su alta densidad de población y fuerte bancarización on line, en general los ataques van dirigidos a aquellas comunidades donde hay una gran densidad de entidades económicas, como bancos, Brasil es el principal destino de los atacantes debido a su alta densidad de población y fuerte bancarización on line. Luego se ubican Uruguay, Argentina, Chile, entre otros por su alta penetración de internet.

A nivel de leyes, Argentina ya cuenta con una normativa sobre delitos informáticos aprobada en 2008, y en 2011 se adhirió al único acuerdo internacional que legisla y aplica una política penal contra la ciber delincuencia.

Asimismo, el gobierno colombiano aprobó en julio de 2011 la creación de un equipo CERT para disminuir los fraudes por internet y fortalecer la ciber seguridad y la ciber defensa. Brasil, Argentina, Chile, Venezuela y Uruguay cuentan con CERT oficiales gubernamentales, por lo que los usuarios deben usar sentido común cuando reciben un correo electrónico sospechoso solicitando sus contraseñas.

- Nunca ingresar al sitio del banco a través de un link, sino que hacerlo directamente a través de la página web de la institución.

[89]PHISHING [en linea] http://www.enlacesbolivia.net/sp/noticias_proc.asp?Seleccion=471#sthash [consulta 24/11/14.]

- Preocuparse por conocer las características y operatorias asociadas a los productos y canales bancarios.
- Resguardar la información personal y particularmente las claves de autentificación y desconfiar si recibe un mail donde le regalan algo.
- Revisar periódicamente las cartolas electrónicas y verificar las transacciones realizadas.
- Mantener siempre un antivirus actualizado.
- No descargar nunca archivos que provengan de correos electrónicos, sobre todo si causan dudas, como si cuentan con faltas de ortografía.(90)

En el Octavo Congreso sobre Prevención del Delito y Justicia Penal, llevado a cabo en 1990 en La Habana, recomendó elaborar normas y directrices sobre la seguridad de las computadoras, para ayudar a la comunidad internacional a hacer frente a estas formas de delincuencia. Además, preparó una lista de delitos informáticos reconocidos por la institución. El manual de las Naciones Unidas para la Prevención y Control de delitos Informáticos señala que, por ser una nueva forma de crimen transnacional, para su combate debe crearse cooperación concertada y resume así los problemas inherentes: 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. 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. En septiembre de 1989, el Comité de Ministros del Consejo Europeo adoptó la

[90] PHISHING [en línea] http://infosurhoy.com/cocoon/saii/xhtml/es/features/saii/features/main/2012/06/08/feature-01 [Consulta 27/11/14].

recomendación sobre delitos informáticos, consignando la importancia de una adecuada y rápida respuesta al nuevo cambio de delincuencia informática. Esta recomendación sienta las bases para una futura coordinación entre la ley y la práctica y mejora de la cooperación internacional. Además, recomienda la investigación, enseñanza y formación, en esta materia. …"La Comisión Europea se ha propuesto proteger la intimidad en las redes, tomando en cuenta los siguientes puntos: a) el riesgo que Internet genera para el derecho a la intimidad y los datos personales, b) el principio de que el uso de datos personales debe reducirse al mínimo c) las condiciones bajo las que los datos personales pueden ser divulgados a terceros, por razones de seguridad nacional o prevención de delitos."(91) En Europa, existe la tendencia de sancionar penalmente los siguientes comportamientos: Fraude en el Campo de la Informática. Falsificación en materia informática. Sabotaje informático y daños a datos computarizados o programas informáticos. Acceso no autorizado. Interceptación sin autorización. Reproducción no autorizada de un programa informático protegido. Espionaje Informático. Uso no autorizado de una computadora. Tráfico de claves informáticas obtenidas por medio ilícito. Distribución de virus o programas delictivos.

Existe consenso sobre de la penalización de estas conductas delictivas generadas por el uso del ordenador. Finalmente, las experiencias legislativas expuestas arrojan los siguientes indicadores: La preocupación mundial se centra en la protección de la información procesada a través del uso de la computadora. En vista de las especiales características de estos delitos, tanto por la forma de comisión, como por la dificultad de rastrear estos casos, algunos países han dispuesto la creación de órganos especializados en la materia. Con el fin de proteger y hacer prevalecer los derechos de los

[91]PALADELLA Carlos [en línea] derecho.org/comunidad/carlospaladella/cps-1.htm [consulta 31/08/14.]

ciudadanos. En los países europeos la inquietud en cuanto al tema data de casi una década atrás. Otros países han seguido de cerca esta actualización con la inclusión de normas similares, aunque con cierto retraso. Distinguimos, en las legislaciones estudiadas, algunas coincidencias en cuanto a la tipificación de conductas delictivas; entre ellas podemos citar falsificación informática, el acceso no autorizado, la destrucción de datos, la infracción del derecho de autor, la interceptación de correo electrónico, las estafas electrónicas. Ahora bien, el análisis realizado nos permite entender que la legislación informática a nivel internacional es un conjunto de regulaciones correctivas dedicadas a normar el problema, no de manera preventiva sino más bien correctiva. En este sentido, el país se halla en una situación de ventaja, pues los niveles de peligrosidad aún no son incontrolables y estamos a tiempo de prevenirlos en base a las experiencias adquiridas por otros Estados.

A continuación hacemos un cuadro en el cual se determina claramente la presencia de tipo penal de falsificación informática en países de Sud América.

| | | |
|---|---|---|
| **ARGENTINA** | Delitos informáticos<br>- Ley 11.179 (Código Penal de la Nación)<br>- Ley 26.388 (Modificación del Código Penal)<br>Otras disposiciones relacionadas<br>- Ley 11.723 (Régimen Legal de la Propiedad | **FALSIFICACIÓNINFORMÁTICA**.<br>Artículo 2.-<br>Será reprimido con prisión de un mes a tres años, siempre que el hecho no constituya un delito más severamente penado, el que ilegítimamente y a sabiendas, alterare de cualquier forma, destruyere, inutilizare, suprimiere o hiciere inaccesible, o de cualquier modo y por cualquier |

| | | |
|---|---|---|
| | Intelectual)<br>Otras leyes<br>- Ley 25.326 (Protección de Datos Personales) Disposiciones específicas<br>- Acceso ilícito: Artículo 153 bis y 157 del Código Penal<br>- Interceptación ilícita: Artículo 153 del Código Penal<br>- Interferencia en los Datos: Artículo 183 y 184 del Código Penal<br>- Interferencia en el Sistema: Artículos 183, 184 y 197 del Código Penal<br>- Abuso de los Dispositivos: Artículo 183 del Código Penal<br>- Falsificación Informática: Artículo 77 del Código Penal y articulo 2.<br>- Fraude Informático: Artículos 172 y 173 | medio, dañare un sistema o dato informático.<br>Artículo 3.-<br>En el caso del artículo 2º, la pena será de dos a ocho años de prisión, si mediara cualquiera de las circunstancias siguientes:<br>1) Ejecutarse el hecho con el fin de impedir el libre ejercicio de la autoridad o en venganza de sus determinaciones;<br>2) Si fuera cometido contra un sistema o dato informático de valor científico, artístico, cultural o financiero de cualquier administración pública, establecimiento público o de uso público de todo género;<br>3) Si fuera cometido contra un sistema o dato informático concerniente a la seguridad, defensa nacional, salud pública o la prestación de servicios públicos. Sí del hecho resultaren, además, lesiones de las descritas en los artículos 90 o 91 del Código Penal, la pena será de tres a quince años de prisión, y si resultare la muerte se elevará hasta veinte años de prisión |

| | | |
|---|---|---|
| | del Código Penal<br>- Pornografía Infantil: Artículo 128 del Código Penal<br>- Infracciones de la Propiedad Intelectual y de los derechos afines: Artículo 71 de la Ley de la Propiedad Intelectual (11.723) | |
| **CHILE** | Delitos informáticos<br>- Ley No. 19.223 relativa a Delito Cibernético<br>Otras disposiciones relacionadas<br>- Ley 19628 Protección Vida Privada y Datos<br>Otras leyes<br>- Ley 18.168 Ley de Telecomunicaciones<br>- Ley-20009<br>Disposiciones Específicas<br>- Acceso ilícito: Artículo 2 de la Ley Relativa a Delitos Informáticos (19.233)<br>- Interceptación ilícita: Artículo 2 de la Ley Relativa a Delitos | **FALSIFICACIÓN INFORMÁTICA**<br>Artículo 2º.- El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.<br><br>Artículo 3º.- El que maliciosamente altere, dañe o destruya los datos contenidos en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.<br><br>Artículo 4º.- El que maliciosamente revele o difunda los datos contenidos en un sistema de información, sufrirá la |

| | | |
|---|---|---|
| | Informáticos (19.233)<br>- Interferencia en los Datos: Artículo 3 de la Ley Relativa a Delitos Informáticos (19.233)<br>- Interferencia en el Sistema: Artículo 1 de la Ley Relativa a Delitos Informáticos (19.233)<br>Derecho Procesal<br>- Procedimientos para la investigación de Delitos Informáticos<br>- Código Procesal Penal<br>Otros procedimientos relacionados<br>- Código Penal Normas Pornografía Infantil<br>Disposiciones Específicas<br>- Registro y Confiscación de datos informáticos almacenados: Artículo 217 y 218 del Código Procesal Penal. | pena de presidio menor en su grado medio. Si quien incurre en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.".<br><br>Y por cuanto he tenido a bien aprobarlo y sancionarlo; por tanto promúlguese y llévese a efecto como Ley de la República |
| **PERU** | Delitos informáticos<br>- Ley N° 30096 - | **FALSIFICACION INFORMATICA.**<br>CAPÍTULO VI |

| | | |
|---|---|---|
| | Delitos Informáticos<br>Disposiciones Específicas<br>- Acceso ilícito: Art. 2 de la Ley N° 30096<br>Interceptación Ilícita: Art. 7 de la Ley N° 30096<br>- Interferencia en los Datos: Art. 3 de la Ley N° 30096<br>- Interferencia en el Sistema: Art. 4 de la Ley N° 30096<br>- Abuso de los Dispositivos: Art. 10 de la Ley N° 30096<br>- Falsificación Informática: Art. 9 de la Ley N° 30096<br>- Fraude Informático: Art. 8 de la Ley N° 30096<br>- Pornografía Infantil: Art. 5 de la Ley N° 30096<br>- Infracciones de la Propiedad Intelectual y de los derechos afines: Art. 8 de la Ley N° 30096<br>Derecho Procesal<br>- Procedimientos para | DELITOS INFORMÁTICOS CONTRA LA FE PÚBLICA<br>Artículo 9. Suplantación de identidad<br>El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio, material o moral, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco año |

| | | |
|---|---|---|
| | la investigación de Delitos Informáticos<br>Código Procesal Penal | |
| **REP. DOMINICANA** | Delitos Informáticos<br>- Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología<br>Disposiciones Específicas<br>- Acceso ilícito: Artículo 6 de la ley 53/07<br>- Interceptación ilícita: Artículo 9 de la Ley 53/07<br>- Interferencia en los Datos: Artículo 10 de la Ley 53/07<br>- Interferencia en el Sistema: Artículo 11 de la Ley 53/07<br>- Abuso de Dispositivos: Artículo 8 de la Ley 53/07<br>- Falsificación Informática: Artículo 18 de la Ley 53/07<br>- Fraude Informático: Artículos 13 - 16 de la Ley 53/07<br>- Pornografía Infantil: Artículo 24 de la Ley | **FALSIFICACIÓN INFORMÁTICA**<br>Articulo 18.- De la Falsedad de Documentos y Firmas. Todo aquel que falsifique, desencripte, decodifique o de cualquier modo descifre, divulgue o trafique, con documentos, firmas, certificados, sean digitales o electrónicos, será castigado con la pena de uno a tres años de prisión y multa de cincuenta a doscientas veces el salario mínimo. |

| | | |
|---|---|---|
| | 53/07<br>- Infracciones de la Propiedad Intelectual y de los Derechos afines: Artículo 25 de la Ley 53/07<br>Derecho Procesal<br>- Procedimientos para la Investigación de Delitos Informáticos<br>- Ley No. 53-07 sobre Crímenes y Delitos de Alta Tecnología<br>Disposiciones Específicas<br>- Conservación Rápida de Datos Informáticos Almacenados: Artículo 54(b) de la Ley 53/07<br>- Conservación y Revelación Parcial rápidas de datos sobre el tráfico: Artículo 56 de la Ley 53/07<br>- Orden de Presentación: Artículo 54(a) de la Ley 53/07<br>- Registro y Confiscación: | |

| | | |
|---|---|---|
| | Artículo 54(b), (e), (f) y (j) de la Ley 53/07<br>- Obtención en tiempo real de datos sobre el tráfico: Artículo 54(k), e (l)de la Ley 53/07<br>- Obtención en tiempo real de datos sobre el contenido: Artículo 54(l) de la Ley 53/07 | |
| **ECUADOR** | Delitos informáticos<br>- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 2002-67)<br>Disposiciones Específicas<br>- Acceso ilícito: Artículo 59, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 2002-67)<br>- Interferencia en los Datos: Artículos 60 y 62, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos | **FALSIFICACIÓN INFORMÁTICA**<br>Artículo 61.- A continuación del Art. 353, agréguese el siguiente artículo enumerado: Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:<br>1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial; |

| | | |
|---|---|---|
| | (Ley No. 2002-67)<br>- Interferencia en el Sistema: Artículos 60 y 62, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 2002-67)<br>- Abuso de Dispositivos: Artículos 63 y 64, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 2002-67)<br>- Falsificación Informática: Artículo 61, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 2002-67)<br>- Fraude Informático: Artículo 61, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 2002-67)<br>- Pornografía Infantil: | 2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;<br>3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.<br><br>El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este capítulo. |

| | | |
|---|---|---|
| | Artículo 528.7 del Código Penal<br>Derecho Procesal<br>- Procedimientos para la investigación de Delitos Informáticos<br>- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos (Ley No. 2002-67)<br>Disposiciones Específicas<br>- Orden de Presentación: Artículo 149 del Código Procesal Penal<br>- Registro y Confiscación de datos informáticos almacenados: Artículo 93 del Código Procesal Penal<br>- Interceptación de Datos sobre el Contenido: Artículos 150 y 155 del Código Procesal Penal. | |
| **PARAGUAY** | Delitos Informáticos<br>- Código Penal Paraguayo – Ley | **FALSIFICACIÓN INFORMÁTICA**<br>Artículo 248.- Alteración de datos relevantes para la prueba |

| | | |
|---|---|---|
| | 1160/97<br>Otras Disposiciones Relacionadas<br>- Ley No. 2861/2006, que Reprime el Comercio y la Difusión Comercial o no Comercial de Material Pornográfico, Utilizando la Imagen u otra Representación de Menores o Incapaces<br>- Ley de Derecho del Autor y Derechos Conexos (Arts. 167 – 170)<br>Disposiciones Específicas<br>- Interceptación ilícita: Artículo 146 del Código Penal<br>- Interferencia en los Datos: Artículo 174 del Código Penal<br>- Interferencia en el Sistema: Artículo 175 del Código Penal<br>- Falsificación Informática: Artículo 248 del Código | 1º El que con la intención de inducir al error en las relaciones jurídicas, almacenara o adulterara datos en los términos del artículo 174, inciso 3º, relevantes para la prueba de tal manera que, en caso de percibirlos se presenten como un documento no auténtico, será castigado con pena privativa de libertad de hasta cinco años o con multa.<br>2º En estos casos será castigada también la tentativa.<br>3º En lo pertinente se aplicará también lo dispuesto en el artículo 246, inciso 4º. |

| | | |
|---|---|---|
| | Penal<br><br>- Fraude Informático: Artículo 188 del Código Penal<br><br>- Pornografía Infantil: Artículo 140 de la Ley 3440/07<br>Derecho Procesal<br>- Procedimientos para la Investigación de Delitos Informáticos<br>- Código Procesal Penal | |

FUENTE: LEGISLACIÓN COMPARADA [en línea] html//remja.oea.com[consulta 11/11/14]

**RESUMEN ANALÍTICO**

Habiendo desarrollado el concepto, la clasificación y habiendo analizado la legislación comparada acerca de la falsificación informática tomamos en cuenta que la cotidianidad de los bolivianos se ve involucrada con el ordenador, que es una realidad permanente en el quehacer diario, queda claro que nuestras leyes vigentes no pueden ser ajenas a este fenómeno que se va desarrollando con el transcurso de los días.

Agregamos, que la dificultad que se experimenta, en nuestra realidad nacional, de prevenir, probar, perseguir, sancionar la falsificación informática, los cuales ocasionan regularmente pérdidas millonarias por la impunidad de los protagonistas. Los artículos referidos a los delitos

informáticos es una ley penal en blanco, la cual no satisface el principio de legalidad. Si la ley es la que define el hecho punible, significa que la misma debe fijar con claridad, precisión y exactitud, el sentido de las palabras y de las cosas, mientras que en estos artículos convergen distintas figuras delictivas.

En si el artículo 7 de la Convención del Consejo de Europa sobre Cibernética, llevado a cabo en Budapest el 27 de noviembre 2001, establece la obligación de los Estados de adoptar todas las medidas, legislativas o de otra especie, para erigir en infracción penal conforme a su derecho interno, la introducción, la alteración, la eliminación y la supresión intencional y contraria a derecho de datos informáticos, la generación de datos no auténticos, con la intención de que ellos sean tenidos en cuento utilizados para fines legales como si fueran auténticos, sean o no directamente legibles o inteligibles. Las parte pueden exigir una intención fraudulenta o una intención delictiva similar como la requerida para la responsabilidad penal.

En la actualidad nuestro país se ve en la necesidad de tipificar la falsificación informática, debido es uno de los delitos más comunes cometidos, los cuales se encuentran en completa impunidad debido a que la actual legislación penal acerca de delitos informáticos es muy general y presenta vacíos legales los cuales son tan notables gracias al desarrollo de la tecnología.

Una medida pronta para evitar más impunidad en el área de los delitos informáticos es incluir en nuestra legislación penal nuevos tipos penales los cuales sean tipificados y sancionados de manera clara y especifica.
Sin embargo en varios países del mundo existe una normativa clara acerca de los delitos informáticos en la cual la falsificación informática y su sanción

a sido considerada como un delito informático más cometido en los últimos veinte años.

Ante la evidente necesidad de reformar nuestro derecho penal, se considera esencial la reforma de nuestro Código Penal vigente, la cual modifique e incorpore nuevos tipos penales como la falsificación informática, en nuestro país es necesaria la creación de una ley en contra de los delitos informáticos la cual este acorde a la necesidad del desarrollo de la tecnología además que la misma ley este basada en organismos, tratados y convenios internacionales.

# ***CONCLUSIONES Y RECOMENDACIONES***

## CAPITULO V

## CONCLUSIONES Y RECOMENDACIONES

### 5.1 CONCLUSIONES

Después de realizar un exhaustivo y cuidadoso análisis del derecho penal, del derecho informático, de los delitos informáticos, para ingresar con la falsificación informática finalmente de las orientaciones del derecho comparado, concluimos afirmando que el legislador boliviano no se puede quedar de brazos cruzados y que debe regular este aspecto planteado acerca de la falsedad informática. La búsqueda de una mejor forma de llenar los vacíos y subsanar las imperfecciones de nuestro ordenamiento sustantivo nos lleva a formularnos las siguientes metas:

1.- Lograr que el avance tecnológico y su correspondiente legislación se desarrollen a la par, que avancen al mismo tiempo.

2.- Reforzar el sistema de justicia penal e involucrar a la sociedad en la prevención de este tipo penal señalado como falsificación informática, especificando el objeto tutelado y la forma de comisión, e incorporando disposiciones precisas que tipifiquen claramente las conductas con relación a la falsificación informática.

3.- Penalizar conductas antisociales, realizadas a través del uso de recursos informáticos, es una exigencia del desarrollo social. En Bolivia, el derecho penal y el derecho en su conjunto deben marcar límites en la conducta de los operadores de sistemas informáticos, mediante la tipificación penal de los comportamientos antisociales que pueden derivarse del uso de medios electrónicos. La revolución digital, como todas las revoluciones, genera incertidumbre pero lo importante es saber responder rápidamente a las exigencias de la vida social, de esto dependerá el futuro del país. Una ley sustantiva de criminal en el área

penal para nuestro país es el primer paso de un proyecto de amplio alcance para colocar a Bolivia a la par de los países desarrollados. Este proyecto es sólo un inicio para la adhesión a la sociedad de la información. De la agilidad con que Bolivia se introduzca dependerá su capacidad para competir con otros Estados. Por lo tanto, una vez que se consolide una legislación acerca de la falsificación informática y otros delitos informáticos existirá una consolidación de la seguridad de nuestra información a fin de generar seguridad jurídica.

4.- La estrategia más adecuada para combatir la falsificación informática debe comprender la coordinación internacional, extensa y específica. En este sentido, se requiere la coordinación legislativa internacional, para evitar los paraísos informáticos equivalentes a los paraísos fiscales; nos referimos a países cuya carencia de normas que regulen estos aspectos los conviertan en atractivos centros para la comisión del delito en cuestión. Soluciones extensas no comprenden tan sólo las legales, sino también la adopción de medidas preventivas como la educación y la misma tecnología. La protección implica además soluciones específicas, para proteger la información a través de normas adecuadas; esto derivará inevitablemente en una nueva doctrina. Una protección y prevención efectiva requiere: Un análisis objetivo de las necesidades de protección y de las fuentes de peligro.

5. Es inminente que los delitos informáticos no se denuncian para evitar alarma; las víctimas prefieren asumir las consecuencias y prevenir en un futuro, a iniciar un proceso judicial; esto se suma a la precariedad y anacronismo del sistema jurídico penal que dificulta la planeación de medidas sancionadoras y preventivas adecuadas.

6. Es urgente superar la insuficiencia de nuestros institutos penales a través de una tipificación detallada de la falsificación informática. Este objetivo es inaplazable.

La hipótesis de esta investigación consistió en La incorporación de la falsificación informática como tipo penal en Bolivia, permitirá una mayor protección al bien jurídicamente protegido de la información, posterior a analizar el concepto de falsificación informática, y la problemática que deviene de éste delito, se demostró de manera indudable que la normativa existente es deficiente, y es este factor principal el que se logra concluir a través del desarrollo de la investigación, lo más preocupante es que no existe un consenso definitivo sobre el tratamiento de esta problemática, es decir, si existiese una normativa consolidada, considero que tal dispersión y omisión normativa provienen a partir de los siguientes factores:

- El Derecho Informático es una rama del derecho cuya regulación e identificación específica es tratada por algunos autores como una necesidad. Precisamente en Bolivia, el Derecho Informático, no ha llegado a esta fase de unificación e identificación, por lo tanto la normativa que lo regula se encuentra en igual sentido dispersa y existe muchos vacíos jurídicos, por lo que debe recurrirse a una integración exhaustiva del derecho para analizar los acontecimientos que se desprenden de éste.
- El desarrollo acelerado de la tecnología crecimiento el cual genera nuevas formas de delincuencia.

- Se han establecido los argumentos doctrinales y sociales por los que se justifica la posibilidad y la viabilidad de la incorporación de la falsificación informática dentro de nuestro actual Código Penal, así como se ha demostrado en la legislación comparada, puesto que la falsificación informática se va desarrollando y generando mayores daños.

7.- En síntesis, se considera necesaria una armonía entre la normativa y la realidad nacional, que no se adscriba simplemente a un discurso de

índole político, sino que consiga efectivamente suplir las necesidades de la sociedad en general.

8.- La legislación es necesaria para evitar abusos y desmanes. Es importante educar a la población respecto a los peligros y formas de prevenir este tipo de delito que es la falsificación informática y de manera especial para los actores de este delito. La labor de educación debe comprender una amplia difusión tanto en las empresas como en las dependencias particulares en general, además de la preparación del personal directamente involucrado en estos delitos, jueces, abogados, empleados de bancos, entre otros. Los jueces carecen de medios para una cabal aplicación e interpretación de la norma. Una correcta tipificación de las conductas ilegales debe ir acompañada de una preparación adecuada para el personal judicial, para estructurar su mente frente a este tipo de situaciones, algunas desconocidas hasta hoy. Hay que desarrollar tecnología más sofisticada para prevenir la falsificación informática y así perfeccionar las medidas de seguridad. Todo este proceso, debe ir acompañado del desarrollo de las experiencias e inteligencia en el campo de investigación de estos delitos. Esto implica la actualización permanente contribuirá, de este modo a la concientización de la comunidad, reforzando la confianza en las autoridades encargadas de aplicar la ley, porque con la capacitación del personal mejoramos su capacidad de investigar y detectar los delitos. En resumen, la lucha contra la delincuencia informática comprende, además de una adecuada legislación, la difusión y la capacitación de personal, con el fin de educar a las potenciales víctimas y estimular denuncias. Es necesario que en Bolivia se prevea en un futuro cercano, la creación de un órgano estatal o supranacional que obtenga la cooperación de todos los usuarios para la prevención del delito de falsificación informática. Un órgano que concentre las denuncias sobre accesos no autorizados a

los sistemas, que no revele la identidad de la víctima y que, sobre la base de esta información, pueda elaborar recomendaciones al usuario común.

## 5.2. RECOMENDACIONES

1.- En primer lugar se debe concientizar sobre el problema y dar a conocer las medidas preventivas, para una política integral contra la falsificación informática se recomienda:

- Elaborar un diagnóstico amplio de la situación de la infraestructura informática nacional.
- Impulsar la concertación de acciones con los diferentes sectores del país. Apoyar la implementación de medidas.
- Realizar un seguimiento de las medidas adoptadas a nivel nacional e internacional para dar solución a esta problemática.
- Organizar foros de análisis de este tema

2.- La actualización de juristas, personal judicial, abogados e interesados mediante una enseñanza integrada y multidisciplinaria capaz de proveer la base técnica indispensablemente para entender el fenómeno de esta nueva era a través de seminarios y cursos participativos. Corresponde a los Estados el brindar medios de seguridad tal y como se hace en la vida real. Este es el desafío que nos propone el nuevo siglo, la creación de leyes destinadas a allanar el camino del progreso. El país no debe limitarse a regular los delitos a medida que éstos surgen, sino crear una institución que se encargue de su investigación o reforzar nuestra Policía Nacional en si es necesario legislar con fines más preventivos, por ende, es imprescindible proponer medidas preventivas destinadas a evitar la expansión de estos delitos.

La respuesta de nuestro país a este fenómeno ha de ser multidireccional y deberá resguardar y preservar la convivencia pacífica de los

ciudadanos, incluyendo una propuesta de módulos educativos en varios niveles para crear en el individuo común la tan deseada cultura de la informática, la falta de control y de una legislación específica permite que se distorsionen las conductas, pues con el sólo conocimiento de que podemos ser juzgados por nuestra conducta, nos limitaremos a actuar en el marco que esa ley señala en si estas leyes deben adecuarse rápidamente porque con el aumento en la cantidad de personas que acceden a una computadora y a Internet, aumenta potencialmente.

3.- En cuanto al carácter transnacional de los delitos informáticos, es preciso crear un ambiente de cooperación y coordinación entre los Estados ya sea al momento de investigar ya sea al momento de aplicar la ley. Se debe unificar criterios, a fin de evitar contradicciones legales delito entre un país y otro, es conveniente suscribir tratados de cooperación para contrarrestar la incidencia de la criminalidad. Consideramos que la privación de la libertad es la sanción adecuada para el delito de falsificación informática por sus especiales características. Las dificultades para encontrar pruebas, debido a la no conciencia entre el delito de falsificación informática y el lugar donde se sufren sus consecuencias, obligan a algunos países a crear departamentos especializados en delincuencia informática, los cuales aprovechan el enorme potencial de la informática para la investigación de estos delitos.

4.- El potencial de la informática para la información, la educación, el entretenimiento y la actividad económica es muy importante. Bolivia requiere una respuesta acorde con esta realidad actual, así es como la actividad legislativa juega un papel importante en la actualización jurídica. En materia penal la tipicidad y legalidad son principios fundamentales e imprescindibles, en esta óptica que las nuevas formas de delincuencia requieren de una regulación específica, evitando el riesgo de caer en la atipicidad. Así, la confección de un apropiado

ordenamiento jurídico beneficiará a nuestra comunidad que armonice las exigencias de información y las garantías del ciudadano.

5.- Una legislación adecuada a la realidad debe tomar en cuenta factores relevantes del problema que genera la falsificación informática.

6.- Asimismo, hay que penar a las personas físicas o jurídicas de carácter privado que manipulen los datos de un tercero con el fin de obtener su información y se vulnere, la economía, el honor, la intimidad personal o familiar del mismo. No existe gradación del sujeto activo, es decir, no se hace diferencia alguna entre el acceso doloso o culposo, y tampoco se menciona qué sucede cuando existen circunstancias ventajosas para la comisión del delito, como en el caso de un empleado de la institución o un encargado del mensaje de sistemas o un funcionario público, cuya sanción deberá ser ejemplarizadora como la inhabilitación especial. Tampoco se especifica un castigo diferente para quien difunda o revele los datos obtenidos.

7.- Deben sancionarse también los actos dañinos o la circulación de material dañino. Debe existir una agravante en el caso de efectuarse los datos contenidos en el sistema de redes o en las computadoras o cuando se afectan a un organismo de defensa nacional, seguridad interior e inteligencia, y aplicarse prisión para estos delitos. Aunque existen otros medios de comisión de la Falsificación Informática, el requisito indispensable es la malicia en el actuar.

8.- Además de las penas establecidas en el Código, hay que establecer medidas alternativas de sanción para la falsificación informática, para resocializar al condenado en el contexto que lo rodea como ser multas, reparación del daño, dependiendo su cuantificación del caso concreto así como del grado de lesión del bien jurídico tutelado.

9.-Es necesaria la implementación de falsificación informática en nuestra legislación penal, debido a la transición de la economía digital donde el dinero y los actos jurídicos empresariales, organizacionales y personales,

desaparecen, transformando los documentos escritos en documentos digitalizados. En este sentido es mayor entonces la razón para proteger la información.

10. En cuanto al procedimiento a llevarse a cabo en caso de la incorporación de la falsificación informática, deberá regirse conforme a lo establecido para los delitos privados a denuncia de la víctima y si es menor de su representante legal, excepto en los casos en que se ve involucrado el Estado.
12. En conclusión, la incorporación de nuevos tipos penales en el área de delitos informáticos debe estar en base al Convenio de Ciber delincuencia realizado en Budapest el año 2001, además que los legisladores deberán revisar legislación de otros países y así lograr que nuestras leyes informáticas tengan más consistencia y especificidad.
13. Se debe establecer una tipificación específica y clara la cual otorgue a todos los usuarios de los ordenadores y terceros la protección integral de manera tal que alcance todos los sectores potencialmente afectados por la falsificación informática.
14. Frente a la falta de regulación específica sugerimos la modificación y complementación del art. 363 del Código Penal, la cual precisará establecer de manera clara los nuevos tipos penales a incorporar en nuestra actual legislación penal de las conductas delictivas.

Ahora bien, en este texto se reunieron aspectos generales de las incidencias de la informática en el derecho, en procura de exponer una visión amplia de la nueva gama de conductas relacionadas con el ordenador. Esta investigación es tan sólo una pequeña parte del universo informática - derecho, porque las discusiones doctrinarias continuarán e involuntariamente algunos detalles no se han toma en cuenta. La protección debe ser integral de manera tal que alcance todos los sectores potencialmente afectados por estos delitos. Frente a la falta de regulación específica sugerimos la

modificación y complementación del artículo. 363 bis y ter del Código Penal,e incluir la falsificación informática. Finalmente, debemos reconocer que las tecnologías de la información forman parte de nuestro desarrollo nacional, en el sector público, privado o social, y que la globalización es un fenómeno insoslayable. La presente investigación plantea un pequeño aporte acerca de cómo enfrentar esta problemática. Vivimos en una época de cambios, en la cual los paradigmas tradicionales se ven reemplazados por nuevos paradigmas. Nuestro sistema socio - cultural es sacudido por constantes transformaciones que dificultan la creación de normas reguladoras de las conductas humanas y de allí surgen situaciones totalmente novedosas, como en el caso de los delitos informáticos. La propuesta de modificación y complementación es acertada, porque actualiza los tipos penales en virtud del principio de legalidad, ya que si bien algunas figuras se adaptan a este tipo de conductas, no ocurre lo mismo con todas.

# ***PROPUESTA DE MODIFICACION DE ARTICULO***

## CAPITULO VI.

## 6.1. PROPUESTA DE MODIFICACIÓN DE ARTÍCULO.

**LEY DE ESTADO PLURINACIONAL**

**EVO MORALES AYMA**

**PRESIDENTE CONSTITUCIONAL DEL ESTADO PLURINACIONAL DE BOLIVIA**

**EN CONSEJO DE MINISTROS DECRETA:**

**LEY DE INCORPORACIÓN DE PARÁGRAFO CUARTO EN EL ARTICULO 363 DE EL CÓDIGO PENAL.**

**ARTICULO UNICO.- Incorpórese el parágrafo cuarto en el articulo 363 del código penal de 11 de marzo de 1997 bajo el siguiente texto:**

**Articulo 363 quater. (FALSIFICACIÓN INFORMÁTICA).-** El que con intención de generar un perjuicio ajeno obteniendo un beneficio para sí o para un tercero altere, borre o suprima datos informáticos que se hallen registrados en sistemas informáticos en cualquier otro tipo de archivo o registro público o privado electrónico, generando datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos con independencia de que sean legibles o inelegibles directamente en perjuicio del titular de los datos o de un tercero será castigado con reclusión de uno a cuatro años

Las penas podrán ser agravadas, si el titular de la información prueba un perjuicio económico. Si los hechos descritos en el artículo anterior fueran cometidos por: Las personas encargadas de los datos, soportes informáticos, la pena se agravará. Los funcionarios públicos o privados que valiéndose de su cargo, serán sancionados con reclusión de 3 años.

**BIBLIOGRAFÍA**

**LIBROS Y REVISTAS.**


1. BACIGALUPO Z. Enrrique. 2002 — "Documentos electrónicos delitos de falsedad documental" Revista electrónica de Ciencia Penal.

.

2. CABANELLAS, Guillermo Editorial 2000 — "Diccionario jurídico elemental" Heliasta S.R.L Buenos Aires Argentina

3. BALBOA Gómez Manuel 2007 — "Phishing falsificación informática " Revista de la Prensa "En Profundidad"

4. CAMPOLI, GABRIEL ANDRES. 2003 — "Nuevas Tendencias Criminológicas Victimológicas en la Sociedad de la Información", en Alfa Redi: Revista de Derecho Informático.

5. CREUS, Carlos. 2004. 2004 — "Derecho Penal. Parte General", Editorial Buenos Aires, Buenos Aires - Argentina

6. DAVARA Rodriguez M. A. 2008 — "Manual de Derecho Informático". Amazadi. Barcelona – España.

7. GARCIA Rivas Nicolás 1996 — "Poder punitivo del estado democrático "Editorial Heliasta Madrid España.

8. JAVIER RIVAS Alejandro, 1999 "Aspectos Jurídicos del Comercio en Internet" Editorial Amanzadi Pamplona – España.

9. MATA Y MARTIN Ricardo 2001 "Delincuencia Informática y Derecho Penal" Editorial Edisofer Madrid - España.

10. MIGUEL HARB, Benjamín 2003 "Derecho Penal", Editorial. Juventud. La Paz – Bolivia.

11. MORENO NAVARRETE Miguel 1999 "Contratos Electrónicos" Editorial Much, Madrid – España.

12. MORALES GUILLEN, Carlos 1999 "Código Penal Concordado y Anotado". Editorial. Gisbert. La Paz – Bolivia

13. MUÑOZ CONDE Francisco 2010 "Derecho Penal" Editorial Rayo del Sur LA Paz – Bolivia.

14. NUÑEZ Ricardo 1987 "Manual de Derecho Penal. " Editorial Heliasta Córdoba - Argentina

15. ORTS Enrique, ROIG Margarita, 2007 "Delitos informáticos y delitos comunes Editorial

16. PAREDES Ana Maria 2008 "Técnicas fáciles de aplicar" Editorial Juventud La Paz – Bolivia.

17. RICO CARRILLO Marilina. 2013 "Los desafíos del derecho Penal frente delitos informáticos y otras conductas fraudulentas en los medios de pago electrónicos" revista del Instituto de Ciencias Jurídicas Puebla - México.

18. SAEZ Capel Jose 2014, "El llamado delito informático no existe" Editorial Rayo del Sur Sucre - Bolivia

19. TÉLLEZ Valdés, Julio. "Derecho Informático", Editorial Mc 1996 Graw Hill. Madrid – España

20. VIEGA MariaJose 2003 "Protección de datos y delitos informáticos" Madrid - España.

**NORMAS LEGALES**

1. CONSTITUCIÓN POLÍTICA DE EL ESTADO texto aprobado por Referendum Constituyente de enero de 2009.
2. CÓDIGO PENAL Ley 1768 de modificaciones al Código Penal de 11 de marzo de 1997.
3. CÓDIGO DE PROCEDIMIENTO PENAL Ley 1970 de 25 de marzo de 1999

**PAGINAS WEB** .

1. AVELEYRA, Antonio 1996, Propuesta Legislativa de Nuevos Tipos Penales en Relación con la Informática, http://www.cddhcu.g...alisco/prop_inf

2. BOTELO Candia Gabriel. “Delitos informáticos” ht4. tp://publicaciones.derecho.org/redp/index.cgi?/N%Famero_4__julio_ de_1999/001.
3. LEVENE, Ricardo, CHIARAVALLOTI, Alicia. “Introducción a los Delitos Informáticos, Tipos y Legislación”. http://www.chiaravalloti_asociados.dtj.com.ar/links_1.htm .
4. PALADELLA Carlos derecho.org/comunidad/carlospaladella/cps-1.htm.
5. WIKIPEDIA 2013 Enciclopedia virtual.

**ANEXO A**

**CONVENIO SOBRE LA CIBER DELINCUENCIA**

**CONSEJO DE EUROPA BUDAPEST (2001)**

Los Estados miembros del Consejo de Europa y los demás Estados signatarios del presente Convenio; Considerando que el objetivo del Consejo de Europa es conseguir una unión más estrecha entre sus miembros; Reconociendo el interés de intensificar la cooperación con los Estados Partes en el presente Convenio;

Convencidos de la necesidad de aplicar, con carácter prioritario, una política penal común encaminada a proteger a la sociedad frente a la ciber delincuencia, entre otras formas, mediante la adopción de la legislación adecuada y el fomento de la cooperación internacional;

Conscientes de los profundos cambios provocados por la digitalización, la convergencia y la globalización continua de las redes informáticas;

Preocupados por el riesgo de que las redes informáticas y la información electrónica sean utilizadas igualmente para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de dichas redes;

Reconociendo la necesidad de una cooperación entre los Estados y el sector privado en la lucha contra la ciberdelincuencia, así como la necesidad de proteger los legítimos intereses en la utilización y el desarrollo de las tecnologías de la información; En la creencia de que la lucha efectiva contra la ciberdelincuencia requiere una cooperación internacional en materia penal reforzada, rápida y operativa; Convencidos de que el presente Convenio resulta necesario para prevenir los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos, mediante la tipificación de esos actos, tal y como se definen en el presente Convenio, y la asunción de poderes suficientes para luchar de forma efectiva contra dichos delitos, facilitando su detección, investigación y sanción, tanto a nivel nacional como internacional, y estableciendo disposiciones que permitan una cooperación internacional rápida y fiable;

Conscientes de la necesidad de garantizar el debido equilibrio entre los intereses de la acción penal y el respeto de los derechos humanos fundamentales consagrados en el Convenio de Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales (1950), el Pacto Internacional de Derechos Civiles y Políticos de las Naciones Unidas (1966) y otros tratados internacionales aplicables en materia de derechos humanos, que reafirman el derecho de todos a defender sus opiniones sin interferencia alguna, así como la libertad de expresión, que comprende la libertad de buscar, obtener y comunicar información e ideas de todo tipo, sin consideración de fronteras, así como el respeto de la intimidad;

Conscientes igualmente del derecho a la protección de los datos personales, tal y como se reconoce, por ejemplo, en el Convenio del Consejo de Europa de 1981 para la protección de las personas con respecto al tratamiento

informatizado de datos personales; Considerando la Convención de las Naciones Unidas sobre los Derechos del Niño (1989) y el Convenio de la Organización Internacional del Trabajo sobre las peores formas de trabajo de los menores (1999); Teniendo en cuenta los convenios existentes del Consejo de Europa sobre cooperación en materia penal, así como otros tratados similares celebrados entre los Estados miembros del Consejo de Europa y otros Estados, y subrayando que el presente Convenio pretende completar dichos Convenios con objeto de dotar de mayor eficacia las investigaciones y los procedimientos penales relativos a los delitos relacionados con los sistemas y datos informáticos, así como facilitar la obtención de pruebas electrónicas de los delitos; Congratulándose de las recientes iniciativas encaminadas a mejorar el entendimiento y la cooperación internacional en la lucha contra la ciber delincuencia, incluidas las medidas adoptadas por las Naciones Unidas, la OCDE, la Unión Europea y el G8; Recordando las recomendaciones del Comité de Ministros nº R (85) 10 relativa a la aplicación práctica del Convenio europeo de asistencia judicial en materia penal, en relación con las comisiones rogatorias para la vigilancia de las telecomunicaciones, nº R (88) 2 sobre medidas encaminadas a luchar contra la piratería en materia de propiedad intelectual y derechos afines, nº R (87) 15 relativa a la regulación de la utilización de datos personales por la policía, sobre la protección de los datos personales en el ámbito de los servicios de telecomunicaciones, con especial referencia a los servicios telefónicos, a sí como sobre la delincuencia relacionada con la informática, que ofrece directrices a los legisladores nacionales para la definición de determinados delitos informáticos, relativa a las cuestiones de procedimiento penal vinculadas a la tecnología de la información;

Teniendo en cuenta la Resolución nº 1, adoptada por los Ministros europeos de Justicia en su XXI Conferencia (Praga, 10 y 11 de junio de 1997), que

recomendaba al Comité de Ministros apoyar las actividades relativas a la ciberde lincuencia desarrolladas por el Comité Europeo de Problemas Penales (CDPC) para aproximar las legislaciones penales nacionales y permitir la utilización de medios de investigación eficaces en materia de delitos informáticos, a sí como la Resolución nº 3, adoptada en la XXIII Conferencia de Ministros europeos de Justicia (Londres, 8 y 9 de junio de 2000), que animaba a las Partes negociadoras a proseguir sus esfuerzos para encontrar soluciones que permitan que el mayor número posible de Estados pasen a ser Partes en el Convenio, y reconocían la necesidad de un sistema rápido y eficaz de cooperación internacional que refleje debidamente las exigencias específicas de la lucha contra la ciber delincuencia;

Teniendo asimismo en cuenta el Plan de Acción adoptado por los Jefes de Estado y de Gobierno del Consejo de Europa con ocasión de su Segunda Cumbre (Estrasburgo, 10 y 11 de octubre de 1997), para buscar respuestas comunes ante el desarrollo de las nuevas tecnologías de la información, basadas en las normas y los valores del Consejo de Europa.

Han convenido en lo siguiente:

Capítulo I - Terminología

Artículo 1 - Definiciones

A los efectos del presente Convenio:

a por sistema informático se entender• todo dispositivo aislado o conjunto de dispositivos interconectados o relacionados entre sÌ, siempre que uno o varios de ellos permitan el tratamiento automatizado de datos en ejecución de un programa;

b por datos informáticos se entender• cualquier representación de hechos, información o conceptos de una forma que permita el

tratamiento informático, incluido un programa diseñado para que un sistema informático ejecute una función;

c por proveedor de servicios se entender:

i toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar por medio de un sistema informático, y

ii cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios de ese servicio;

d por datos sobre el tráfico se entender cualesquiera datos informáticos relativos a una comunicación por medio de un sistema informático, generados por un sistema informático como elemento de la cadena de comunicación, que indiquen el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación o el tipo de servicio subyacente.

Capítulo II - Medidas que deben adoptarse a nivel nacional

Sección 1 - Derecho penal sustantivo

Título 1 - Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

Artículo 2 - Acceso ilícito

Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a la totalidad o a una parte de un sistema informático. Cualquier Parte podrá exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos o con otra intención delictiva, o en relación con un sistema informático que esté conectado a otro sistema informático.

Artículo 3 - Interceptación ilícita

Cada Parte adoptar las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la interceptación

deliberada e ilegítima, por medios técnicos, de datos informáticos comunicados en transmisiones no públicas efectuadas a un sistema informático, desde un sistema informático o dentro del mismo, incluidas las emisiones electromagnéticas procedentes de un sistema informático que contenga dichos datos informáticos. Cualquier Parte podrá• exigir que el delito se haya cometido con intención delictiva o en relación con un sistema informático conectado a otro sistema informático.

Artículo 4 - Interferencia en los datos

1 Cada Parte adoptar las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de actos que dañen, borren, deterioren, alteren o supriman datos informáticos.

2 Cualquier Parte podrá• reservarse el derecho a exigir que los actos definidos en el apartado provoquen daños graves.

Artículo 5 - Interferencia en el sistema

Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, provocación de daños, borrado, deterioro, alteración o supresión de datos informáticos.

Artículo 6 - Abuso de los dispositivos

1 Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a. la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de:

i un dispositivo, incluido un programa informático, diseñado o adaptado principalmente para la comisión de cualquiera de los delitos previstos de conformidad con los anteriores artículo 2 a 5;

ii una contraseña, un código de acceso o datos informáticos

similares que permitan tener acceso a la totalidad o a una parte de un sistema informático, con el fin de que sean utilizados para la comisión de cualquiera de los delitos contemplados en los artículo 2 a 5; y

b. la posesión de alguno de los elementos contemplados en los anteriores apartados i) o ii) con el fin de que sean utilizados para cometer cualquiera de los delitos previstos en los artículo 2 a 5. Cualquier Parte podrá• exigir en su derecho interno que se posea un número determinado de dichos elementos para que se considere que existe responsabilidad penal.

2. No podrá interpretarse que el presente artículo impone responsabilidad penal en los casos en que la producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición mencionadas en el apartado 1 del presente artículo no tengan por objeto la comisión de un delito previsto de conformidad con los artículo 2 a 5 del presente Convenio, como es el caso de las pruebas autorizadas o de la protección de un sistema informático.

3. Cualquier Parte podrá reservarse el derecho a no aplicar lo dispuesto en el apartado 1 del presente artículo, siempre que la reserva no afecte a la venta, la distribución o cualquier otra puesta a disposición de los elementos indicados en el apartado 1.a.ii) del presente artículo.

Título 2 - Delitos informáticos

Artículo 7 - Falsificación informática

Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno, cuando se cometa de forma deliberada e ilegítima, la introducción, aliteración, borrado o supresión de datos informáticos que dé lugar a datos no auténticos, con la intención de que sean tenidos en cuenta o utilizados a efectos legales como si se tratara de datos auténticos, con independencia de que los datos sean o no directamente legibles e inteligibles. Cualquier Parte podrá• exigir que

exista una intención fraudulenta o una intención delictiva similar para que se considere que existe responsabilidad penal.

Artículo 8 - Fraude informática

Cada Parte adoptar las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen un perjuicio patrimonial a otra persona mediante:

a cualquier introducción, aliteración, borrado o supresión de datos informáticos;

b cualquier interferencia en el funcionamiento de un sistema informática, con la intención fraudulenta o delictiva de obtener ilegítimamente un beneficio económico para uno mismo o para otra persona.

Título 3 - Delitos relacionados con el contenido

Articulo 9 - Delitos relacionados con la pornografía infantil

1. Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la comisión deliberada e ilegítima de los siguientes actos:

a. la producción de pornografía infantil con vistas a su difusión por medio de un sistema informática;

b la oferta o la puesta a disposición de pornografía infantil por medio de un sistema informático;

c la difusión o transmisión de pornografía infantil por medio de un sistema informático,

d la adquisición de pornografía infantil por medio de un sistema informático para uno mismo o para otra persona;

e la posesión de pornografía infantil en un sistema informático o en un medio de almacenamiento de datos informáticos.

2 A los efectos del anterior apartado 1, por pornografía infantil se entender todo material pornográfico que contenga la representación visual de:

a un menor comportándose de una forma sexualmente explícitas;

b una persona que parezca un menor comportándose de una forma Sexualmente explícitas;

c imágenes realistas que representen a un menor comportándose de una Forma sexualmente explícitas.

3. A los efectos del anterior apartado 2, por menor se entender• toda persona menor de 18 años. No obstante, cualquier Parte podrá• establecer un límite de edad inferior, que ser como mínimo de 16 años.

4. Cualquier Parte podrá reservarse el derecho a no aplicar, en todo o en parte, las letras d) y e) del apartado 1, y las letras b) y c) del apartado 2.

Título 4 - Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

Artículo 10 - Delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines

1. Cada Parte adoptar las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las infracciones de la propiedad intelectual, según se definan en la legislación de dicha Parte, de conformidad con las obligaciones asumidas en aplicación del Acta de París de 24 de julio de 1971 por la que se revise el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre la propiedad intelectual, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

2. Cada Parte adoptar las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno las

infracciones de los derechos afines definidas en la legislación de dicha Parte, de conformidad con las obligaciones que Esta haya asumido en aplicación de la Convención Internacional sobre la protección de los artistas intérpretes o ejecutantes, los productores de fonogramas y los organismos de radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre las obras de los intérpretes y ejecutantes y los fonogramas, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando esos actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.

3. En circunstancias bien delimitadas, cualquier Parte podrá• reservarse el derecho a no exigir responsabilidad penal en virtud de los apartados 1 y 2 del presente artículo, siempre que se disponga de otros recursos efectivos y que dicha reserva no vulnere las obligaciones internacionales que incumban a dicha Parte en aplicación de los instrumentos internacionales mencionados en los apartados 1 y 2 del presente articulo.

TÌtulo 5 - Otras formas de responsabilidad y de sanciones

Artículo 11 - Tentativa y complicidad

1. Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten

   necesarias para tipificar como delito en su derecho interno cualquier complicidad intencionada con vistas a la comisión de alguno de los delitos previstos de conformidad con los artículo 2 a 10 del presente Convenio, con la intensión de que se cometa ese delito.

2. Cada Parte adoptar las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno cualquier tentativa de comisión de alguno de las delitos previstos de

conformidad con los artículos 3 a 5, 7, 8, 9. 1. a) y c) del presente Convenio, cuando dicha tentativa sea intencionada.

3. Cualquier Estado podrá reservarse el derecho a no aplicar, en todo o en parte, el apartado 2 del presente artículos.

Articulo 12 - Responsabilidad de las personas jurídicas

1 Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten necesarias para que pueda exigirse responsabilidad a las personas jurídicas por los delitos previstos de conformidad con el presente Convenio, cuando sean cometidos por cuenta de las mismas por cualquier persona física, tanto en calidad individual como en su condición de miembro de un Órgano de dicha persona jurídica, que ejerza funciones directivas en la misma, en virtud de:

a un poder de representación de la persona jurídica;

b una autorización para tomar decisiones en nombre de la persona jurídica;

c una autorización para ejercer funciones de control en la persona

jurídica.

2. Además de los casos ya previstos en el apartado 1 del presente artículo, cada.

Parte adoptar las medidas necesarias para asegurar que pueda exigirse responsabilidad a una persona jurídica cuando la falta de vigilancia o de control por parte de una persona física mencionada en el apartado 1 haya hecho posible la comisión de un delito previsto de conformidad con el presente Convenio en beneficio de dicha persona jurídica por una persona física que actúe bajo su autoridad.

3 Con sujeción a los principios jurídicos de cada Parte, la responsabilidad de una persona jurídica podrá ser penal, civil o administrativa.

4 Dicha responsabilidad se entender• sin perjuicio de la responsabilidad penal de las personas físicas que hayan cometido el delito.

Artículo 13 - Sanciones y medidas

1 Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten necesarias para que los delitos previstos de conformidad con los artículo 2 a 11 puedan dar lugar a la aplicación de sanciones efectivas, proporcionadas y disuasorias, incluidas penas privativas de libertad.

2 Cada Parte garantizar• la imposición de sanciones o de medidas penales o no penales efectivas, proporcionadas y disuasorias, incluidas sanciones pecuniarias, a las personas jurídicas consideradas responsables de conformidad con el articulo 12.

Sección 2 - Derecho procesal

artículo 14 - ámbito de aplicación de las disposiciones sobre procedimiento

1. Cada Parte adoptar las medidas legislativas y de otro tipo que resulten necesarias para establecer los poderes y procedimientos previstos en la presente Sección para los fines de investigaciones o procedimientos penales específicos.

2 Salvo que se establezca específicamente otra cosa en el artículo 21, cada Parte aplicar• los poderes y procedimientos mencionados en el apartado 1 del presente artículo a:

a los delitos previstos de conformidad con los artículo 2 a 11 del presente Convenio;

b otros delitos cometidos por medio de un sistema informático; y

c la obtención de pruebas electrónicas de un delito.

3. A Cualquier Parte podrá• reservarse el derecho a aplicar las medidas indicadas en el articulo 20 exclusivamente a los delitos o categorías de delitos especificados en la reserva, siempre que el •ámbito de dichos delitos o categorías de delitos no sea más reducido que el de los delitos a los que esa Parte aplique las medidas indicadas en el articulo

21. Las Partes procurarán limitar dichas reservas para permitir la aplicación más amplia posible de la medida indicada en el articulo 20.

b Cuando, como consecuencia de las limitaciones existentes en su legislación vigente en el momento de la adopción del presente Convenio, una Parte no pueda aplicar las medidas indicadas en los artÌculos 20 y 21 a las comunicaciones transmitidas en el sistema informático de un proveedor de servicios:

i utilizado en beneficio de un grupo restringido de usuarios, y

ii que no utilice las redes públicas de comunicaciones ni esté

Conectado a otro sistema informático, ya sea público o privado, dicha Parte podrá reservarse el derecho a no aplicar dichas medidas a esas comunicaciones. Cada Parte procurar limitar este tipo de reservas de forma que se permita la aplicación más amplia posible de las medidas indicadas en los artículo 20 y 21.

Artículo 15 - Condiciones y salvaguardas

1 Cada Parte se asegurar de que el establecimiento, la ejecución y la aplicación de los poderes y procedimientos previstos en la presente sección estén sujetas a las condiciones y salvaguardas previstas en su derecho interno, que deber garantizar una protección adecuada de los derechos humanos y de las libertades, incluidos los derechos derivados de las obligaciones asumidas en virtud del Convenio del Consejo de Europa para la protección de los derechos humanos y las libertades fundamentales (1950), del Pacto Internacional de derechos civiles y políticos de las Naciones Unidas (1966), y de otros instrumentos internacionales aplicables en materia de derechos humanos, y que deber• integrar el principio de proporcionalidad.

2 Cuando resulte procedente dada la naturaleza del procedimiento o del poder de que se trate, dichas condiciones incluirán, entre otros aspectos, la supervisión judicial u otra forma de supervisión independiente, los motivos que justifiquen la aplicación, y la limitación

del •ámbito de aplicación y de la duración del poder o del procedimiento de que se trate.

3 Siempre que sea conforme con el interés público y, en particular, con la correcta administración de la justicia, cada Parte examinar• la repercusión de los poderes y procedimientos previstos en la presente sección en los derechos, responsabilidades e intereses legítimos de terceros.

Título 2 - Conservación rápida de datos informáticas almacenados

Artículo 16 - Conservación rápida de datos informáticas almacenados

1 Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten necesarias para permitir a sus autoridades competentes ordenar o imponer de otra manera la conservación rápida de determinados datos electrónicos, incluidos los datos sobre el tráfico, almacenados por medio de un sistema informático, en particular cuando existan razones para creer que los datos informáticas resultan especialmente susceptibles de pérdida o de modificación.

2 Cuando una Parte aplique lo dispuesto en el anterior apartado 1 por medio de una orden impartida a una persona para conservar determinados datos almacenados que se encuentren en posesionó o bajo el control de dicha persona, la Parte adoptar• las medidas legislativas y de otro tipo que resulten necesarias para obligar a esa persona a conservar y a proteger la integridad de dichos datos durante el tiempo necesario, hasta un máximo de noventa día, de manera que las autoridades competentes puedan conseguir su revelación. Las Partes podrán prever que tales Órdenes sean renovables.

3 Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten necesarias para obligar al encargado de la custodia de los datos o a otra persona encargada de su conservación a mantener en secreto la aplicación de dichos procedimientos durante el plazo previsto en su derecho interno.

4 Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículo 14 y 15.

Artículo 17 - Conservación y revelación parcial rápidas de datos sobre el tráfico

1 Para garantizar la conservación de los datos sobre el trafico en aplicación de lo dispuesto en el articulo 16, cada Parte adoptar las medidas legislativas y de otro tipo que resulten necesarias:

a para asegurar la posibilidad de conservar rápidamente dichos datos sobre el tráfico con independencia de que en la transmisión de esa comunicación participaran uno o varios proveedores de servicios, y

b para garantizar la revelación rápida a la autoridad competente de la Parte, o a una persona designada por dicha autoridad, de un volumen suficiente de datos sobre el tráfico para que dicha Parte pueda identificar a los proveedores de servicio y la vía por la que se transmití la comunicación.

2 Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículo 14 y 15.

Título 3 - Orden de presentación

artículo 18 - Orden de presentación

1 Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar:

a una persona que se encuentre en su territorio que comunique determinados datos informáticos que posea o que se encuentren bajo su control, almacenados en un sistema informático o en un medio de almacenamiento de datos informáticos; y

b a un proveedor de servicios que ofrezca prestaciones en el territorio de esa Parte que comunique los datos que posea o que se encuentren bajo su control relativos a los abonados en conexión con dichos servicios.

2 Los poderes y procedimientos mencionados en el presente articulo estén sujetos a lo dispuesto en los artículo 14 y 14.

3 A los efectos del presente artículo, por datos relativos a los abonados de Entender toda información, en forma de datos informáticos o de cualquier otra forma, que posea un proveedor de servicios y esté relacionada con los abonados a dichos servicios, excluidos los datos sobre el trafico o sobre el contenido, y que permita determinar:

a el tipo de servicio de comunicaciones utilizado, las disposiciones técnicas adoptadas al respecto y el periodo de servicio;

b la identidad, la direccione postal o geográfica y el número de teléfonos del abonado, así como cualquier otro número de acceso o información sobre facturación y pago que se encuentre disponible sobre la base de un contrato o de un acuerdo de prestación de servicios;

c cualquier otra información relativa al lugar en que se encuentren los equipos de comunicaciones, disponible sobre la base de un contrato o de un acuerdo de servicios.

Título 4 - Registro y confiscación de datos informáticas almacenados

artículo 19 - Registro y confiscación de datos informáticas almacenados

1 Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a registrar o a tener acceso de una forma similar:

a a un sistema informático o a una parte del mismo, así como a los datos Informáticos almacenados en el mismo; y

b a un medio de almacenamiento de datos informáticos en el que puedan almacenarse datos informáticos, en su territorio.

2 Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten necesarias para asegurar que, cuando sus autoridades procedan al registro o tengan acceso de una forma similar a un sistema informático específico o a una parte del mismo, de

conformidad con lo dispuesto en el apartado 1.a, y tengan razones para creer que los datos buscados estén almacenados en otro sistema informático o en una parte del mismo situado en su territorio, y dichos datos sean lícitamente accesibles a través del sistema inicial o estén disponibles para Esté, dichas autoridades puedan ampliar rápidamente el registro o la forma de acceso similar al otro sistema.

3 Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten

necesarias para facultar a sus autoridades competentes a confiscar o a obtener de una forma similar los datos informáticos a los que se haya tenido acceso en aplicación de lo dispuesto en los apartados 1 Û 2. Estas medidas incluirán las siguientes facultades:

a confiscar u obtener de una forma similar un sistema informático o una parte del mismo, o un medio de almacenamiento de datos informáticos;

b realizar y conservar una copia de dichos datos informáticos;

c preservar la integridad de los datos informáticos almacenados de que se trate;

d hacer inaccesibles o suprimir dichos datos informáticos del sistema informático al que se ha tenido acceso.

4 Cada Parte adoptar las medidas legislativas y de otro tipo que resulten necesarias para facultar a sus autoridades competentes a ordenar a cualquier persona que conozca el funcionamiento del sistema informático o las medidas aplicadas para proteger los datos informáticos contenidos en el mismo que facilite toda la información necesaria, dentro de lo razonable, para permitir la aplicación de las medidas indicadas en los apartados 1 y 2.

5 Los poderes y procedimientos mencionados en el presente artÌculo estarán sujetos a lo dispuesto en los artículo 14 y 15.

Título 5 - Obtención en tiempo real de datos informáticos

Artículo 20 - Obtención en tiempo real de datos sobre el tráfico

1 Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten

Necesarias para facultar a sus autoridades competentes a:

a obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, y

b obligar a un proveedor de servicios, dentro de los limites de su capacidad técnica

i a obtener o grabar mediante la aplicación de medios técnicos existentes en su territorio, o

ii a prestar a las autoridades competentes su colaboración y su asistencia para obtener o graba en tiempo real los datos sobre el tráfico asociados a comunicaciones específicas transmitidas en su territorio por medio de un sistema

2 Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá• adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el tráfico asociados a determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.

3 Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten

necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4 Los poderes y procedimientos mencionados en el presente artículo estarán sujetos a lo dispuesto en los artículos 14 y 15.

Artículo 21 - Interceptación de datos sobre el contenido

1 Cada Parte adoptar las medidas legislativas y de otro tipo que resulten necesarias para facultar a las autoridades competentes, por lo que respecta a una serie de delitos graves que deberán definirse en su derecho interno:

a a obtener o a grabar mediante la aplicación de medios técnicos existentes en su territorio, y

b a obligar a un proveedor de servicios, dentro de los límites de su capacidad técnica:

i a obtener o a grabar mediante la aplicación de los medios técnicos existentes en su territorio, o

ii a prestar a las autoridades competentes su colaboración y su asistencia para obtener o graba en tiempo real los datos sobre el contenido de determinadas comunicaciones en su territorio, transmitidas por medio de un sistema informática.

2 Cuando una Parte, en virtud de los principios consagrados en su ordenamiento jurídico interno, no pueda adoptar las medidas indicadas en el apartado 1.a), podrá adoptar en su lugar las medidas legislativas y de otro tipo que resulten necesarias para asegurar la obtención o la grabación en tiempo real de los datos sobre el contenido de determinadas comunicaciones transmitidas en su territorio mediante la aplicación de los medios técnicos existentes en el mismo.

3 Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten necesarias para obligar a un proveedor de servicios a mantener en secreto el hecho de que se ha ejercido cualquiera de los poderes previstos en el presente artículo, así como toda información al respecto.

4 Los poderes y procedimientos mencionados en el presente artículo estará sujetos a lo dispuesto en los artículo 14 y 15.

Sección 3 - Jurisdicción

artículo 22 - Jurisdicción

1 Cada Parte adoptar• las medidas legislativas y de otro tipo que resulten necesarias para afirmar su jurisdicción respecto de cualquier delito previsto con arreglo a los artículos 2 a 11 del presente Convenio, siempre que se haya cometido:

a en su territorio; o

b a bordo de un buque que enarbole pabellón de dicha Parte; o

c a bordo de una aeronave matriculada según las leyes de dicha Parte; o

d por uno de sus nacionales, si el delito es susceptible de sanción penal en el lugar en el que se cometió o si ningún Estado tiene competencia territorial respecto del mismo.

2 Cualquier Estado podrá reservarse el derecho a no aplicar o a aplicar Únicamente en determinados casos o condiciones las normas sobre jurisdicción establecidas en los apartados 1.b) a 1.d) del presente artículo o en cualquier otra parte de los mismos.

3 Cada Parte adoptar las medidas que resulten necesarias para afirmar su jurisdicción respecto de los delitos mencionados en el apartado 1 del articulo 24 del presente Convenio, cuando el presunto autor del delito se encuentre en su territorio y no pueda ser extraditado a otra Parte por razón de su nacionalidad, previa solicitud de extradición.

4 El presente Convenio no excluye ninguna jurisdicción penal ejercida por una Parte de conformidad con su derecho interno.

5 Cuando varias Partes reivindiquen su jurisdicción respecto de un presunto delito contemplado en el presente Convenio, las Partes interesadas celebrarán consultas, siempre que sea oportuno, con miras a determinar cuál es la jurisdicción más adecuada para las actuaciones penales.

Título 1 - Principios generales relativos a la cooperación internacional

Artículo 23 - Principios generales relativos a la cooperación internacional

Las Partes cooperarán entre sÌ en la mayor medida posible, de conformidad con las disposiciones del presente capítulo, en aplicación de los instrumentos internacionales aplicables a la cooperación internacional en materia penal, de acuerdos basados en legislación uniforme o recíproca y de su derecho interno, para los fines de las investigaciones o los procedimientos relativos a los delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas electrónicas de los delitos.

Título 2 - Principios relativos a la extradición

Artículo 24 - Extradición

1 a El presente artículo se aplicar a la extradición entre las Partes por los delitos establecidos en los artículo 2 a 11 del presente Convenio, siempre que estén castigados en la legislación de las dos Partes implicadas con una pena privativa de libertad de una duración máxima de como mínimo un año, o con una pena más grave.

b Cuando deba aplicarse una pena mínima diferente en virtud de un acuerdo basado en legislación uniforme o recíproca o de un tratado de extradición aplicable entre dos o más Partes, incluido el Convenio Europeo de Extradición (STE nº 24), se aplicar la pena mínima establecida en virtud de dicho acuerdo o tratado.

2 Se considerar que los delitos mencionados en el apartado 1 del presente artículo están incluidos entre los delitos que dan lugar a extradición en cualquier tratado de extradición vigente entre las Partes. Las Partes se comprometen a incluir dichos delitos entre los que pueden dar lugar a extradición en cualquier tratado de extradición que puedan celebrar entre sí.

3 Cuando una Parte que condicione la extradición a la existencia de un tratado reciba una solicitud de extradición de otra Parte con la que no haya celebrado ningún tratado de extradición, podrá• aplicar el presente Convenio como fundamento jurídico de la extradición

respecto de cualquier delito mencionado en el apartado 1 del presente artículo.

4 Las Partes que no condicionen la extradición a la existencia de un tratad reconocer• n los delitos mencionados en el apartado 1 del presente artículo como delitos que pueden dar lugar a extradición entre ellas.

5 La extradición estar sujeta a las condiciones establecidas en el derecho interno de la Parte requerida o en los tratados de extradición aplicables, incluidos los motivos por los que la Parte requerida puede denegar la extradición.

6 Cuando se deniegue la extradición por un delito mencionado en el apartado 1 del presente artículo únicamente por razón de la nacionalidad de la persona buscada o porque la Parte requerida se considera competente respecto de dicho delito, la Parte requerida deber• someter el asunto, a petición de la Parte requirente, a sus autoridades competentes para los fines de las actuaciones penales pertinentes, e informar• a su debido tiempo del resultado final a la Parte requirente. Dichas autoridades tomaron su decisión y efectuarán sus investigaciones y procedimientos de la misma manera que para cualquier otro delito de naturaleza comparable, de conformidad con la legislación de dicha Parte.

7 a Cada Parte comunicar al Secretario General del Consejo de Europa, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, el nombre y la dirección de cada autoridad responsable del envío o de la recepción de solicitudes de extradición o de detención provisional en ausencia de un tratado.

b El Secretario General del Consejo de Europa crear y mantendrá• actualizado un registro de las autoridades designadas por las Partes. Cada

Parte garantizar en todo momento la exactitud de los datos que figuren en el registro.

Título 3 - Principios generales relativos a la asistencia mutua

artículo 25 - Principios generales relativos a la asistencia mutua

1 Las Partes se concederán asistencia mutua en la mayor medida posible para los fines de las investigaciones o procedimientos relativos a delitos relacionados con sistemas y datos informáticos o para la obtención de pruebas en formato electrónico de un delito.

2 Cada Parte adoptar también las medidas legislativas y de otro tipo que resulten necesarias para cumplir las obligaciones establecidas en los artículo 27 a 35.

3 En casos de urgencia, cada Parte podrá• transmitir solicitudes de asistencia o comunicaciones relacionadas con las mismas por medios rápidos de comunicación, incluidos el fax y el correo electrónico, en la medida en que dichos medios ofrezcan niveles adecuados de seguridad y autenticación (incluido el cifrado, en caso necesario), con confirmación oficial posterior si la Parte requerida lo exige. La Parte requerida aceptar• la solicitud y dar• respuesta a la misma por cualquiera de estos medios rápidos de comunicación.

4 Salvo que se establezca específicamente otra cosa en los artículos del presente capítulo, la asistencia mutua estar• sujeta a las condiciones previstas en el derecho interno de la Parte requerida o en los tratados de asistencia mutua aplicables, incluidos los motivos por los que la Parte requerida puede denegar la cooperación. La Parte requerida no ejercer• el derecho a denegar la asistencia mutua en relación con los delitos mencionados en los artículos 2 a 11 ˙nicamente porque la solicitud se refiere a un delito que considera de naturaleza fiscal.

5 Cuando, de conformidad con las disposiciones del presente capítulo, se permita a la Parte requerida condicionar la asistencia mutua a la existencia de una doble tipificación penal, dicha condición se

considerar• cumplida cuando la conducta constitutiva del delito respecto del cual se solicita la asistencia constituya un delito en virtud de su derecho interno, con independencia de que dicho derecho incluya o no el delito dentro de la misma categoría de delitos o lo denomine o no con la misma terminología que la Parte requirente,.

artículo 26 - Información espontánea

1 Dentro de los límites de su derecho interno, y sin petición previa, una Parte podrá• comunicar a otra Parte información obtenida en el marco de sus propias investigaciones cuando considere que la revelación de dicha información podría ayudar a la Parte receptora a iniciar o llevar a cabo investigaciones o procedimientos en relación con delitos previstos en el presente Convenio o podría dar lugar a una petición de cooperación de dicha Parte en virtud del presente capítulo.

2 Antes de comunicar dicha información, la Parte que la comunique podrá solicitar que se preserve su confidencialidad o que se utilice con sujeción a determinadas condiciones. Si la Parte receptora no puede atender esa solicitud, informar• de ello a la otra Parte, que deber• entonces determinar si a pesar de ello debe facilitarse la información o no. Si la Parte destinataria acepta la información en las condiciones establecidas, quedar• vinculada por las mismas.

Titulo 4 - Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

artículo 27 - Procedimientos relativos a las solicitudes de asistencia mutua en ausencia de acuerdos internacionales aplicables

1 Cuando entre las Partes requirente y requerida no se encuentre vigente un tratado de asistencia mutua o un acuerdo basado en legislación uniforme o recíproca, serán de aplicación las disposiciones de los apartados 2 a 10 del presente articulo. Las disposiciones del presente articulo no serán de aplicación cuando exista un tratado, acuerdo o legislación de este tipo, salvo que las Partes interesadas convengan en

aplicar en su lugar la totalidad o una parte del resto del presente articulo.

2 aCada Parte designar una o varias autoridades centrales encargadas de enviar solicitudes de asistencia mutua y de dar respuesta a las mismas, de su ejecución y de su remisión a las autoridades competentes para su ejecución.

b Las autoridades centrales se comunicarán directamente entre sí.

c En el momento de la firma o del deposito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte comunicar• al Secretario General del Consejo de Europa los nombres y direcciones de las autoridades designadas en cumplimiento del presente apartado.

d El Secretario General del Consejo de Europa crear y mantendrá actualizado un registro de las autoridades centrales designadas por las Partes. Cada Parte garantizar• en todo momento la exactitud de los datos que figuren en el registro.

3 Las solicitudes de asistencia mutua en virtud del presente articulo se ejecutarán de conformidad con los procedimientos especificados por la Parte requirente, salvo que sean incompatibles con la legislación de la Parte requerida.

4 Además de las condiciones o de los motivos de denegación contemplados en el apartado 4 del artículo 25, la Parte requerida podrá• denegar la asistencia si:

a la solicitud se refiere a un delito que la Parte requerida considera delito político o delito vinculado a un delito político;

b la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

5 La Parte requerida podrá• posponer su actuación en respuesta a una solicitud cuando dicha actuación pudiera causar perjuicios a

investigaciones o procedimientos llevados a cabo por sus autoridades.

6 Antes de denegar o posponer la asistencia, la Parte requerida estudiar•, previa consulta cuando proceda con la Parte requirente, si puede atenderse la solicitud parcialmente o con sujeción a las condiciones que considere necesarias.

7 La Parte requerida informar• sin demora a la Parte requirente del resultado de la ejecución de una solicitud de asistencia. Deber• motivarse cualquier denegación o aplazamiento de la asistencia solicitada. La Parte requerida informar• también a la Parte requirente de cualquier motivo que haga imposible la ejecución de la solicitud o que pueda retrasarla de forma significativa.

8 La Parte requirente podrá solicitar a la Parte requerida que preserve la confidencialidad de la presentación de una solicitud en virtud del presente capítulo y del objeto de la misma, salvo en la medida necesaria para su ejecución. Si la Parte requerida no puede cumplir esta petición de confidencialidad, lo comunicar• inmediatamente a la Parte requirente, que determinar• entonces si pese a ello debe procederse a la ejecución de la solicitud.

9 a En casos de urgencia, las solicitudes de asistencia mutua o las comunicaciones al respecto podrán ser enviadas directamente por las autoridades judiciales de la Parte requirente a las autoridades correspondientes de la Parte requerida. En tal caso, se enviar• al mismo tiempo copia a la autoridad central de la Parte requerida a través de la autoridad central de la Parte requirente.

b Cualquier solicitud o comunicación en virtud de este apartado podr• Efectuarse a través de la Organización Internacional de Policía Criminal (INTERPOL).

c Cuando se presente una solicitud en aplicación de la letra a) del presente articulo y la autoridad no sea competente para tramitarla,

remitir• la solicitud a la autoridad nacional competente e informar• directamente a la Parte requirente de dicha remisión.

d Las solicitudes y comunicaciones efectuadas en virtud del presente apartado que no impliquen medidas coercitivas podrán ser remitidas directamente por las autoridades competentes de la Parte requirente a las autoridades competentes de la Parte requerida.

e En el momento de la firma o el deposito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Parte podrá• informar al Secretario General del Consejo de Europa de que, por razones de eficacia, las solicitudes formuladas en virtud del presente apartado deben dirigirse a su autoridad central.

artículo 28 - Confidencialidad y restricción de la utilización

1 En ausencia de un tratado de asistencia mutua o de un acuerdo basado en legislación uniforme o recíproca que esté vigente entre las Partes requirente y requerida, serán de aplicación las disposiciones del presente articulo. Las disposiciones del presente artículo no serán de aplicación cuando exista un tratado, acuerdo o legislación de este tipo, salvo que las Partes interesadas convengan en aplicar en su lugar la totalidad o una parte del resto del presente articulo.

2 La Parte requerida podrá supeditar la entrega de información o material e respuesta a una solicitud a la condición de que:

a se preserve su confidencialidad cuando la solicitud de asistencia judicial mutua no pueda ser atendida en ausencia de esta condición, o

b no se utilicen para investigaciones o procedimientos distintos de los indicados en la solicitud.

3 Si la Parte requirente no puede cumplir alguna condición de las mencionadas en el apartado 2, informar• de ello sin demora a la otra Parte, que determinar• en tal caso si pese a ello debe facilitarse la

información. Cuando la Parte requirente acepte la condición, quedar• vinculada por ella.

4 Cualquier Parte que facilite información o material con sujeción a una condición con arreglo a lo dispuesto en el apartado 2 podrá• requerir a la otra Parte que explique, en relaciona con dicha condición, el uso dado a dicha información o material.

Sección 2 - Disposiciones especiales

Título 1 - Asistencia mutua en materia de medidas provisionales

Articulo 29 - Conservación rápida de datos informáticos almacenados

1 Una Parte podrá• solicitar a otra Parte que ordene o asegure de otra forma la conservación rápida de datos almacenados por medio de un sistema informática que se encuentre en el territorio de esa otra Parte, respecto de los cuales la Parte requirente tenga la intención de presentar una solicitud de asistencia mutua con vistas al registro o al acceso de forma similar, la confiscación o la obtención de forma similar, o la revelación de los datos.

2 En las solicitudes de conservación que se formulen en virtud del apartado 1 se indicar:

a la autoridad que solicita dicha conservación;

b el delito objeto de investigación o de procedimiento penal y un breve resumen de los hechos relacionados con el mismo;

c los datos informáticos almacenados que deben conservarse y su relaciona con el delito

d cualquier información disponible que permita identificar a la persona encargada de la custodia de los datos informáticos almacenados o la ubicación del sistema informática;

e la necesidad de la conservación; y

f que la Parte tiene la intención de presentar una solicitud de asistencia mutua para el registro o el acceso de forma similar, la

confiscación o la obtención de forma similar o la revelación de los datos informáticos almacenados.

3 Tras recibir la solicitud de otra Parte, la Parte requerida tomar• las medidas adecuadas para conservar rápidamente los datos especificados de conformidad con su derecho interno. A los efectos de responder a una solicitud, no se requerir• la doble tipificación penal como condición para proceder a la conservación.

4 Cuando una Parte exija la doble tipificación penal como condición para atender una solicitud de asistencia mutua para el registro o el acceso de forma similar, la confiscación o la obtención de forma similar o la revelación de datos almacenados, dicha Parte podrá• reservarse, en relaciona con delitos distintos de los previstos con arreglo a los artículo 2 a 11 del presente Convenio, el derecho a denegar la solicitud de conservación en virtud del presente artículo en los casos en que tenga motivos para creer que la condición de la doble tipificación penal no podrá cumplirse en el momento de la revelación.

5 Asimismo, las solicitudes de conservación únicamente podrán denegarse si:

a la solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político;

b la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

6 Cuando la Parte requerida considere que la conservación por sí sola no bastar para garantizar la futura disponibilidad de los datos o pondrá• en peligro la confidencialidad de la investigación de la Parte requirente o causar• cualquier otro perjuicio a la misma, informar de ello sin demora a la Parte requirente, la cual decidir• entonces si debe pese a ello procederse a la ejecución de la solicitud.

7 Las medidas de conservación adoptadas en respuesta a la solicitud mencionada en el apartado 1 tendrán una duración mínima de sesenta día, con objeto de permitir a la Parte requirente presentar una solicitud de registro o de acceso de forma similar, confiscación u obtención de forma similar, o de revelación de los datos. Cuando se reciba dicha solicitud, seguirán conservándose los datos hasta que se adopte una decisión sobre la misma.

artículo 30 - Revelación rápida de datos conservados sobre el tráfico

1 Cuando, con motivo de la ejecución de una solicitud presentada de conformidad con el articulo 29 para la conservación de datos sobre el tráfico en relación con una comunicación específica, la Parte requerida descubra que un proveedor de servicios de otro Estado participó en la transmisión de la comunicación, la Parte requerida revelar• rápidamente a la Parte requirente un volumen suficiente de datos sobre el tráfico para identificar al proveedor de servicios y la vìa por la que se transmití la comunicación.

2 La revelación de datos sobre el tráfico en virtud del apartado 1 ˙nicamente podrá denegarse si:

a la solicitud hace referencia a un delito que la Parte requerida considera delito político o delito relacionado con un delito político;

b la Parte requerida considera que la ejecución de la solicitud podría atentar contra su soberanía, seguridad, orden público u otros intereses esenciales.

Título 2 - Asistencia mutua en relación con los poderes de investigación

artículo 31 - Asistencia mutua en relación con el acceso a datos informáticos almacenados

1 Una Parte podrá• solicitar a otra Parte que registre o acceda de forma similar, confisque u obtenga de forma similar y revele datos almacenados por medio de un sistema informático situado en el

territorio de la Parte requerida, incluidos los datos conservados en aplicación del artículo 29.

2 La Parte requerida dar• respuesta a la solicitud aplicando los instrumentos internacionales, acuerdos y legislación mencionados en el articulo 23, así como de conformidad con otras disposiciones aplicables en el presente capítulo.

3 Se dar• respuesta lo antes posible a la solicitud cuando:

a existan motivos para creer que los datos pertinentes están especialmente expuestos al riesgo de pérdida o modificación; o

b los instrumentos, acuerdos o legislación mencionados en el apartado 2 prevean la cooperación rápida.

Articulo 32 - Acceso transfronterizo a datos almacenados, con consentimiento o cuando estén a disposición del público Una Parte podrá, sin la autorización de otra Parte:

a tener acceso a datos informáticos almacenados que se encuentren a disposición del público (fuente abierta), con independencia de la ubicación geográfica de dichos datos; o

b tener acceso o recibir, a través de un sistema informático situado en su territorio, datos informáticos almacenados situados en otra Parte, si la Parte obtiene el consentimiento lícito y voluntario de la persona legalmente autorizada para revelar los datos a la Parte por medio de ese sistema informático.

Artículo 33 - Asistencia mutua para la obtención en tiempo real de datos sobre el tráfico

1 Las Partes se prestarán asistencia mutua para la obtención en tiempo real de datos sobre el tráfico asociados a comunicaciones específicas en su territorio transmitidas por medio de un sistema informático. Con sujeción a lo dispuesto en el apartado 2, dicha asistencia se regir por las condiciones y procedimientos establecidos en el derecho interno.

2 Cada Parte prestar dicha asistencia como mínimo respecto de los delitos por los que se podría conseguir la obtención en tiempo real de datos sobre el tráfico en un caso similar en su país.

Artículo 34 - Asistencia mutua relativa a la interceptación de datos sobre el contenido Las Partes se prestaran asistencia mutua para la obtención o grabación en tiempo real de datos sobre el contenido de comunicaciones específicas transmitidas por medio de un sistema informático en la medida en que lo permitan sus tratados y el derecho interno aplicables.

Artículo 35 - 1 Cada Parte designar un punto de contacto disponible las veinticuatro horas del día, siete día a la semana, con objeto de garantizar la prestación de ayuda inmediata para los fines de las investigaciones o procedimientos relacionados con delitos vinculados a sistemas y datos informáticos, o para la obtención de pruebas electrónicas de un delito. Dicha asistencia incluir• los actos tendentes a facilitar las siguientes medidas o su adopción directa, cuando lo permitan la legislación y la práctica internas:

a el asesoramiento técnico;

b la conservación de datos en aplicación de los artículo 29 y 30;

c la obtención de pruebas, el suministro de información jurídica y la localización de sospechosos.

2 a El punto de contacto de una Parte estar• capacitado para mantener comunicaciones con el punto de contacto de otra Parte con carácter urgente.

b Si el punto de contacto designado por una Parte no depende de la autoridad o de las autoridades de dicha Parte responsables de la asistencia mutua internacional o de la extradición, el punto de contacto velar• por garantizar la coordinación con dicha autoridad o autoridades con carácter urgente.

3 Cada Parte garantizar• la disponibilidad de personal debidamente formado y equipado con objeto de facilitar el funcionamiento de la red.

Capítulo IV - Disposiciones finales

artículo 36 - Firma y entrada en vigor

1 El presente Convenio estar abierto a la firma de los Estados miembros del Consejo de Europa y de los Estados no miembros que hayan participado en su elaboración.

2 El presente Convenio estar sujeto a ratificación, aceptación o aprobación.

Los instrumentos de ratificación, aceptación o aprobación se depositaron en poder del Secretario General del Consejo de Europa.

3 El presente Convenio entrar• en vigor el primer día del mes siguiente a la

expiración de un plazo de tres meses desde la fecha en que cinco Estados, de los cuales tres como mínimo sean Estados miembros del Consejo de Europa, hayan expresado su consentimiento para quedar vinculados por el Convenio de conformidad con lo dispuesto en los apartados 1 y 2.

4 Respecto de cualquier Estado signatario que exprese más adelante su consentimiento para quedar vinculado por el Convenio, Éste entrar en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que haya expresado su consentimiento para quedar vinculado por el Convenio de conformidad con lo dispuesto en los apartados 1 y 2.

Articulo 37 - Adhesión al Convenio

1 Tras la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa, previa consulta con los Estados Contratantes del Convenio y una vez obtenido su consentimiento unánime, podrá invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo y que no haya participado en su elaboración. La decisión se adoptar por la mayoría establecida en el artículo 20.d) del

Estatuto del Consejo de Europa y con el voto unánime de los representantes con derecho a formar parte del Comité de Ministros.

2 Para todo Estado que se adhiera al Convenio de conformidad con lo dispuesto en el anterior apartado 1, el Convenio entrar• en vigor el primer dÌa del mes siguiente a la expiración de un plazo de tres meses desde la fecha del depósito del instrumento de adhesión en poder del Secretario General del Consejo de Europa.

Artículo 38 - Aplicación territorial

1 En el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, cada Estado podrá• especificar el territorio o territorios a los que se aplicar• el presente Convenio.

2 En cualquier momento posterior, mediante declaración dirigida al Secretario General del Consejo de Europa, cualquier Parte podrá• hacer extensiva la aplicación del presente Convenio a cualquier otro territorio especificado en la declaración. Respecto de dicho territorio, el Convenio entrar• en vigor el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la declaración.

3 Toda declaración formulada en virtud de los dos apartados anteriores podrá• retirarse, respecto de cualquier territorio especificado en la misma, mediante notificación dirigida al Secretario General del Consejo de Europa. La retirada surtir• efecto el primer día del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido dicha notificación.

Artículo 39 - Efectos del Convenio

1 La finalidad del presente Convenio es completar los tratados o acuerdos multilaterales o bilaterales aplicables entre las Partes, incluidas las disposiciones de:

- el Convenio europeo de extradición, abierto a la firma en Parísel 13 de diciembre de 1957 (STE nº 24);
- el Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 20 de abril de 1959 (STE nº 30);
- el Protocolo adicional al Convenio europeo de asistencia judicial en materia penal, abierto a la firma en Estrasburgo el 17 de marzo de 1978 (STE nº 99).

2 Si dos o más Partes han celebrado ya un acuerdo o tratado sobre las materias reguladas en el presente Convenio o han regulado de otra forma sus relaciones al respecto, o si lo hacen en el futuro, tendrán derecho a aplicar, en lugar del presente Convenio, dicho acuerdo o tratado o a regular dichas relaciones en consonancia. No obstante, cuando las Partes regulen sus relaciones respecto de las materias contempladas en el presente Convenio de forma distinta a la establecida en el mismo, deben hacerlo de una forma que no sea incompatible con los objetivos y principios del Convenio.

3 Nada de lo dispuesto en el presente Convenio afectar• a otros derechos,

Restricciones, obligaciones y responsabilidades de las Partes.

Artículo 40 - Declaraciones

Mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a la facultad de exigir elementos complementarios según lo dispuesto en los artículo 2, 3, 6.1.b), 7,9.3 y 27.9.e).

Artículo 41 - Cláusula federal

1 Los Estados federales podrán reservarse el derecho a asumir las obligaciones derivadas del capítulo II del presente Convenio de forma compatible con los principios fundamentales por los que se rija la

relación entre su gobierno central y los estados que lo formen u otras entidades territoriales análogas, siempre que siga estando en condiciones de cooperar de conformidad con el capítulo III.

2 Cuando formule una reserva en aplicación del apartado 1, un Estado federal no podrá• aplicar los términos de dicha reserva para excluir o reducir el capítulo II. En todo caso, deber dotarse de una capacidad amplia y efectiva que permita la aplicación de las medidas previstas en dicho capítulo.

3 Por lo que respecta a las disposiciones del presente Convenio cuya aplicación sea competencia de los estados federados o de otras entidades territoriales análogas que no estén obligados por el sistema constitucional de la federación a la adopción de medidas legislativas, el gobierno federal informar• de esas disposiciones a las autoridades competentes de dichos estados, junto con su opinión favorable, alentándoles a adoptar las medidas adecuadas para su aplicación.

Artículo 42 - Reservas

Mediante notificación por escrito dirigida al Secretario General del Consejo de Europa, cualquier Estado podrá• declarar, en el momento de la firma o del depósito de su instrumento de ratificación, aceptación, aprobación o adhesión, que se acoge a una o varias de las reservas previstas en el apartado 2 del artículo 4, apartado 3 del artículo 6, apartado 4 del artículo 9, apartado 3 del artículo 10, apartado 3 del artículo 11, apartado 3 del artículo 14, apartado 2 del artículo 22, apartado 4 del artículo 29 y apartado 1 del artículo 41. No podrán formularse otras reservas.

Artículo 43 - Situación de las reservas y retirada de las mismas

1 La Parte que haya formulado una reserva de conformidad con el articulo 42 podrá retirarla en todo o en parte mediante notificación dirigida al Secretario General del Consejo de Europa. Dicha retirada surtir efecto en la fecha en que el Secretario General reciba la

notificación. Si en la notificación se indica que la retirada de una reserva surtir efecto en una fecha especificada en la misma y Ésta es posterior a la fecha en que el Secretario General reciba la notificación, la retirada surtir efecto en dicha fecha posterior.

2 La Parte que haya formulado una reserva según lo dispuesto en el artículo 42 retirar dicha reserva, en todo o en parte, tan pronto como lo permitan las circunstancias.

3 El Secretario General del Consejo de Europa podrá• preguntar periódicamente a las Partes que hayan formulado una o varias reservas según lo dispuesto en el artículo 42 acerca de las perspectivas de que se retire dicha reserva.

Artículo 44 - Enmiendas

1 Cualquier Estado Parte podrá proponer enmiendas al presente Convenio, que serán comunicadas por el Secretario General del Consejo de Europa a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio así como a cualquier Estado que se haya adherido al presente Convenio o que haya sido invitado a adherirse al mismo de conformidad con lo dispuesto en el artículo 37.

2 Las enmiendas propuestas por una Parte serán comunicadas al Comité Europeo de Problemas Penales (CDPC), que presentar al Comité de Ministros su opinión sobre la enmienda propuesta.

3 El Comité de Ministros examinar la enmienda propuesta y la opinión presentada por el CDPC y, previa consulta con los Estados Partes no miembros en el presente Convenio, podrá adoptar la enmienda.

4 El texto de cualquier enmienda adoptada por el Comité de Ministros de conformidad con el apartado 3 del presente artículo ser remitido a las Partes para su aceptación.

5 Cualquier enmienda adoptada de conformidad con el apartado 3 del presente artículo entrar• en vigor treinta día después de que las Partes hayan comunicado su aceptación de la misma al Secretario General.

Artículo 45 - Solución de controversias

1 Se mantendrá• informado al Comité Europeo de Problemas Penales del Consejo de Europa (CDPC) acerca de la interpretación y aplicación del presente Convenio.

2 En caso de controversia entre las Partes sobre la interpretación o aplicación del presente Convenio, Éstas intentarán resolver la controversia mediante negociaciones o por cualquier otro medio pacifico de su elección, incluida la sumisión de la controversia al CDPC, a un tribunal arbitral cuyas decisiones serán vinculantes para las Partes o a la Corte Internacional de Justicia, según acuerden las Partes interesadas.

Artículo 46 - Consultas entre las Partes

1 Las Partes se consultaron periódicamente, según sea necesario, con objeto de facilitar:

a la utilización y la aplicación efectivas del presente Convenio, incluida la detección de cualquier problema derivado del mismo, así como los efectos de cualquier declaración o reserva formulada de conformidad con el presente Convenio;

b el intercambio de información sobre novedades significativas de carácter jurídico, político o tecnológico relacionadas con la ciber delincuencia y con la obtención de pruebas en formato electrónico;

c el estudio de la conveniencia de ampliar o enmendar el presente

2 Se mantendrá periódicamente informado al Comité Europeo de Problemas Penales (CDPC) acerca del resultado de las consultas mencionadas en el apartado 1.

3 Cuando proceda, el CDPC facilitar• las consultas mencionadas en el apartado 1 y tomar• las medidas necesarias para ayudar a las Partes en sus esfuerzos por ampliar o enmendar el Convenio. Como máximo tres anos después de la entrada en vigor del presente Convenio, el Comité Europeo de Problemas Penales (CDPC) llevar• a cabo, en cooperación con las Partes, una revisión de todas las disposiciones del Convenio y, en caso necesario, recomendar• las enmiendas procedentes.

4 Salvo en los casos en que sean asumidos por el Consejo de Europa, los gastos realizados para aplicar lo dispuesto en el apartado 1 serán sufragados por las Partes en la forma que estas determinen.

5 Las Partes contarán con la asistencia de la Secretaría del Consejo de Europa para desempeorar sus funciones en aplicación del presente articulo.

Articulo 47 - Denuncia

1 Cualquier Parte podrá• denunciar en cualquier momento el presente Convenio mediante notificación dirigida al Secretario General del Consejo de Europa.

2 Dicha denuncia surtir efecto el primer dia del mes siguiente a la expiración de un plazo de tres meses desde la fecha en que el Secretario General haya recibido la notificación.

ArtÌculo 48 - Notificación

El Secretario General del Consejo de Europa notificar• a los Estados miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado que se haya adherido al mismo o que haya sido invitado a hacerlo:

a cualquier firma;

b el depósito de cualquier instrumento de ratificación, aceptación, aprobación o adhesión;

c cualquier fecha de entrada en vigor del presente Convenio de conformidad con los artículos 36 y 37;

d cualquier declaración formulada en virtud del articulo 40 o reserva formulad de conformidad con el artículo 42;

e cualquier otro acto, notificación o comunicación relativo al presente Convenio. En fe de lo cual, los infrascritos, debidamente autorizados a tal fin, firman el presente Convenio.

Hecho en Budapest, el 23 de noviembre de 2001, en francés e inglés, siendo ambos textos igualmente auténticos, en un ejemplar que se depositar en los archivos del Consejo de Europa. El Secretario General del Consejo de Europa remitir• copias certificadas a cada uno de los Estados Miembros del Consejo de Europa, a los Estados no miembros que hayan participado en la elaboración del presente Convenio y a cualquier Estado invitado a adherirse al mismo.

**ANEXO B**

**CUESTIONARIO**

EDAD:……..

CARGO QUE

OCUPA:.....……

1.- ¿QUE SON PARA USTED LOS DELITOS INFORMÁTICOS?

……

……

2.- ¿SEGÚN USTED A QUE AFECTAN LOS DELITOS INFORMÁTICOS?

……

……

3.- ESTA USTED DE ACUERDO QUE SE INCORPORE EN EL CÓDIGO PENAL EL TIPO PENAL DE LA FALSIFICACIÓN INFORMÁTICA?

:……

……

4.-¿CUALES SERIAN DESDE SU PUNTO DE VISTA LOS EFECTOS POSITIVOS DE LA INCORPORACIÓN DE FALSIFICACIÓN INFORMÁTICA COMO TIPO PENAL EN EL ACTUAL CÓDIGO PENAL DE BOLIVIA?

:……

……

6.-¿ES VIABLE LA INCORPORACIÓN DE EL TIPO PENAL DE FALSIFICACIÓN INFORMÁTICA EN EL CÓDIGO PENAL?

:……

……