UNIVERSIDAD NACIONAL DE LOJA

MODALIDAD DE ESTUDIOS A DISTANCIA

CARRERA DE DERECHO

TITULO:

"INSUFICIENTE NORMATIVA EN EL CÓDIGO PENAL, SOBRE LOS DELITOS INFORMÁTICOS Y LA FALSIFICACIÓN INFORMÁTICA, EN CUANTO A LOS TIPOS PENALES Y LAS SANCIONES".

TESIS PREVIA A OPTAR EL TITULO DE ABOGADO

AUTOR: Ángelo Antonio Sánchez Maldonado

DIRECTOR: Dr. Mg. Sc. Jefferson Vicente Armijos Gallardo

LOJA - ECUADOR

2013

CERTIFICACIÓN

Dr. Mg. Sc. Jefferson Vicente Armijos Gallardo, Docente de la Carrera de Derecho de la Modalidad de Estudios a Distancia de la Universidad Nacional de Loja,

CERTIFICO:

Que el trabajo de investigación intitulado: *" INSUFICIENTE NORMATIVA EN EL CÓDIGO PENAL, SOBRE LOS DELITOS INFORMÁTICOS Y LA FALSIFICACIÓN INFORMÁTICA, EN CUANTO A LOS TIPOS PENALES Y LAS SANCIONES "*, presentado por el señor Angelo Antonio Sánchez Maldonado, para optar por el título de Abogado, ha sido dirigido, orientado y debidamente revisado, por lo que autorizo su presentación y sustentación pública.

Loja, 6 de diciembre del 2013

Atentamente,

Dr. Mg. Sc. Jefferson Vicente Armijos Gallardo

AUTORÍA

Yo Ángelo Antonio Sánchez Maldonado declaro ser autor(a) del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales, por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi tesis en el repositorio Institucional-biblioteca Virtual.

AUTOR: Ángelo Antonio Sánchez Maldonado

FIRMA: .....

CÉDULA: 1103471247

FECHA: Loja, diciembre del 2013

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo, Ángelo Antonio Sánchez Maldonado declaro ser autor (a) de la Tesis titulada: INSUFICIENTE NORMATIVA EN EL CODIGO PENAL, SOBRE LOS DELITOS INFORMATICOS Y LA FALSIFICACION INFORMATICA, EN CUANTO A LOS TIPOS PENALES Y LAS SANCIONES. Como requisito para optar al Grado de: ABOGADO: autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el Repositorio Digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la Tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los 06 días del mes de diciembre del dos mil trece, firma la autora.

FIRMA:.....

AUTOR: Ángelo Antonio Sánchez Maldonado
CÉDULA: 1103471247
DIRECCIÓN: Loja, Pasaje Sinchona 09-56 y Rocafuerte
CORREO ELECTRÓNICO: dc.angelosma@hotmail.com
TELÉFONO: 2588248 CÉLULAR: 0985985854

DATOS COMPLEMENTARIOS

DIRECTOR DE TESIS: Dr. Jefferson Vicente Armijos Gallardo Mg. Sc.

TRIBUNAL DE GRADO:

Dr. Gonzalo Aguirre Valdivieso Mg. Sc. (Presidente)
Dr. Mario Chacha Vázquez Mg. Sc. (Vocal)
Dr .Igor Vivanco Muller Mg. Sc. (Vocal)

AGRADECIMIENTO

Quiero dejar constancia de mi especial agradecimiento a la Universidad Nacional de Loja, a la Modalidad de Estudios a Distancia, Carrera de Derecho, representadas tan dignamente por sus autoridades, por el apoyo brindado a los estudiantes para realizarse profesionalmente, a todos y cada uno de los maestros por sus conocimientos impartidos y su ardua labor de formación de nosotros sus estudiantes.

Dentro de mis años de preparación académica, he recibido el apoyo incondicional de los seres que forman parte de mi existir sin los cuales no podría culminar mi preparación y los objetivos como profesional en la rama del derecho por lo tanto debo manifestar mi agradecimiento.

Un agradecimiento especial al Director de Tesis, el Dr. Mg. Sc. Jefferson Vicente Armijos Gallardo, por su dedicación, responsabilidad, apoyo y sabias orientaciones, que han permitido culminar el presente trabajo de investigación.

Ángelo Antonio Sánchez Maldonado

DEDICATORIA

El presente trabajo investigativo, lo dedico con todo cariño a mi madre ya que gracias a su apoyo y esfuerzo incondicional he podido realizarme como profesional.

A mi esposa, ejemplo de vida y amiga incondicional, quien con sus consejos y principios morales me ha hecho cada día un mejor ser humano.

A mis hijos, que cada día me han dado la fuerza necesaria para llegar a cumplir otro objetivo en mi vida.

A todos ellos muchas gracias.

Angelo Antonio Sánchez Maldonado

ESQUEMA DE CONTENIDOS

Índice

1.- TITULO

INSUFICIENTE NORMATIVA EN EL CÓDIGO PENAL, SOBRE LOS DELITOS INFORMÁTICOS Y LA FALSIFICACIÓN INFORMÁTICA, EN CUANTO A LOS TIPOS PENALES Y LAS SANCIONES

2.- RESUMEN

La Informática está en su apogeo, un beneficio para todos, en especial, en cuanto a que más y más personas, acuden a la Informática para estar a la par del progreso tecnológico. Una realidad muy acertada y óptima en el desarrollo de nuestro país, pero el problema se suscita cuando "…el avance de la informática y su uso en casi todas las áreas de la vida social, posibilita, cada vez más, el uso de la computación como medio para cometer delitos" de alteraciones, modificaciones, falsificaciones de documentos informáticos, sin que exista una legislación capaz de regular este fenómeno.

La problemática de los delitos informáticos y de la falsificación informática, en nuestro medio, se suscita hace 12 años aproximadamente, desde que la tecnología y en especial la informática toman auge e influencia en su uso, como herramienta de trabajo en distintos sectores y ámbitos, en los cuales se guarda información pública y privada, tanto de personas naturales como jurídicas.

Es por eso, que su tratamiento debe regirse en base a una normativa legal, que se pretende elaborar después del estudio del tiempo y espacio, donde se suscitan los delitos informáticos.

La normativa penal referente al tema de mi plan de tesis, establece: "Art. 353.1.- Falsificación electrónica.- Son reos de falsificación electrónica la persona o personas que con el 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 encuentren contenida en cualquier soporte material, sistema de información o telemático, ya sea: 1. Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial; 2. Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad; 3. Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho", lo cual resulta insuficiente a la hora de establecer o relacionar el delito que se comete, con la norma legal existente, y aún resulta más ridícula la sanción que se fija en el mismo Art. 353.1, inciso 2 que sostiene: "El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo", claramente se observa la ineficiente legislación que a este tema se le ha dado, ya que siendo de interés general los delitos informáticos y la falsificación informática, no hay la teoría en cuanto a lo que son y las respectivas sanciones.

ABSTRACT

Informatics is at its peak, a benefit for all, especially in that more and more people flock to the Computer to keep pace of technological progress. A very successful and actually possible in the development of our country, but the problem arises when "... the advancement of information technology and its use in almost all areas of social life, possible, increasingly, the use of computers as a means to commit crimes "of alteration, modification, falsification of documents computer, with no legislation can regulate this phenomenon.

The problem of cybercrime and related forgery, in our environment, is raised about 12 years ago, since the technology and especially computers gained in popularity and influence in its use as a tool in various sectors and areas, in which public and private information stores, both natural and legal persons.

That's why your treatment should be governed on the basis of legal rules, that might be drawn after the study of time and space, where cybercrime arise.

The criminal law relating to the subject of my thesis plan states: "Art 353.1. - Counterfeit electronics. - Electronic forgery are guilty of the

person or persons to profit or to cause injury to a third party, by any means, alter or modify data messages, or information embedded in them, that are contained in any tangible medium or electronic information system, either: 1. Altering a data message on one of its elements or formal requirements or essential 2. Simulating a data message in whole or in part, so as to mislead as to its authenticity, 3. Assuming an act the involvement of people who have not had or attributing to those who have participated in the act, representations or statements other than those who have made ", which is insufficient in establishing or relating to the offense being commits, with the existing statute, and is even more ridiculous the penalty is set at the same Section 353.1, subsection 2, which states: "The crime of electronic forgery will be punished according to the provisions of this Chapter", clearly legislation inefficient observed this issue has been given as being of general interest and cybercrime related forgery, no theory as to what they are and the respective penalties.

3.- INTRODUCCIÓN

El avance de la tecnología en la Informática, ha permitido el desarrollo de una gran cantidad de elementos, necesarios en la vida y obra del ser humano actual. Constituye lo que denominamos una herramienta, necesaria en la consecución de un sinnúmero de actividades, tales son: gubernativas, legislativas, militares, judiciales, laborales, económicas, educativas, culturales, personales y sociales en general, propias de la actualidad y enmarcadas dentro del proceso evolutivo del hombre. Pero así como constituye un gran progreso, advierto también un resultado negativo, que a través de las tecnologías informáticas, se ha abierto el camino y las puertas al nacimiento y masificación de conductas antisociales y delictivas. Además, a través o en los sistemas informáticos, se han creado nuevas, complicadas y fáciles oportunidades de infringir la ley, y a su vez, han posibilitado lamentablemente, el cometimiento de delitos, los llamados delitos informáticos.

La presente investigación se enmarca, en la apertura al conocimiento y hacer énfasis en la serie de delitos informáticos que se perpetran, además de la clasificación traída por la doctrina jurídica; y, dentro de estos poner de manifiesto al delito de falsificación informática, comprendida con sus tipos penales, así como el establecimiento de

sanciones específicas que caractericen a esta infracción en el Código Penal. Precisamente, las conductas criminales cometidas mediante y dirigidas a los sistemas informáticos, normalmente se dirigen a atacar informaciones, datos, archivos, etc; a estas conductas se las denomina: virus, estafa informática, spamming, falsificación informática, entre otras. Ilícitos claramente conceptualizados, en los cuales el comportamiento delincuencial informático en estas prácticas, van desde una simple intromisión no autorizada en los datos personales de un sujeto, hasta la posible destrucción de todo un sistema informático de una entidad pública o privada.

En virtud de la serie de acontecimientos, noticias, evidencias, que la prensa ha difundido, reflejando que los delitos informáticos en los últimos tiempos van incrementándose de manera alarmante, ha incentivado y propiciado el interés por investigar tales conductas y la respectiva tipificación en los cuerpos legales vigentes en el país. Partiendo de la experiencia del panorama mundial, este tipo de conductas en países cercanos, prácticamente se han visto en la obligación de hacer una adecuación típica de esas conductas, con el fin de evitar su propagación. En nuestro país, se ha hecho difícil para las autoridades encargadas de la investigación y acusación, impulsar una adecuación típica, pues falta herramientas jurídicas adecuadas, para regular las acciones enmarcadas

dentro del ámbito informático, en especial la falsificación informática, que dentro del Código Penal, se observa la carencia del elemento punible.

Es por tales motivos, que existe una gran motivación en hacer de este tema, un mecanismo necesario e importante, y por consiguiente que se encuentre en apogeo en el conocimiento de la población, sobre la posibilidad de ser un sujeto pasivo o víctima y las consecuencias graves de estas conductas ilícitas. Además de por fin, contar con un ordenamiento, una normativa clara que posibilite a las entidades encargadas del juzgamiento, hacer una adecuada administración de justicia en este tema.

Teóricamente hablando, a este tema lo podríamos catapultar dentro de la generación de procesos legislativos que, a través de técnicas adecuadas a cada artículo, norma, posibiliten una reforma o amplitud de la misma, permitiendo la adecuación típica del mayor número de dichos delitos, para que así, el sistema penal sea conforme a las restricciones impuestas por el régimen de los derechos constitucionales y fundamentales. De este modo y, en especial la falsificación informática, alcanzaría el nivel esperado de ley penal, puesto que el propio Código Penal consagra lo establecido sobre la tipicidad de la ley, es decir que nadie puede sufrir una pena que no esté en ella establecida. Asimismo, no se puede actuar

como suelen hacer las autoridades encargadas de investigar este tipo de conductas, cuando no tienen un tipo penal perfectamente aplicable, moldean la conducta a través de una distorsión de supuestos de hecho presentados al fiscal, para que así tal conducta pertenezca a un tipo penal, cuyos principios fácticos no permiten la aplicación de los supuestos, y en el cual, ni siquiera la intención del legislador al tipificar la conducta es aplicable al comportamiento investigado.

El presente proyecto de investigación, se acentúa en una labor investigativa de campo, abierta, directa con los actores y la bibliográfica, destinada a abordar tanto en noticias nacionales como en obras y legislaciones extranjeras, que con sus enseñanzas, nos ayudan al tratamiento y a cubrir en lo posible, el mayor número de dudas que actualmente existe, y que nos enfrentamos casi a diario en nuestras actividades, en especial las dedicadas al sector financiero (entidades bancarias), donde se están produciendo el mayor número de ilícitos de falsificaciones informáticas de instrumentos privados (tarjetas de crédito/débito).

En este panorama, se ha empezado desde la observación de hechos y situaciones cometidos a través y en contra de tecnologías informáticas, de ahí que se ha establecido los antecedentes de la materia en estudio, la

Informática, y enseguida sobre sus ramificaciones, la Telemática, la Informática Jurídica y el Derecho Informático. Después y concretamente se pasa analizar al Delito en general, y dentro de este el Delito Informático, su Clasificación, Sujetos Pasivo y Activo, la Delincuencia Informática y el Bien Jurídico Protegido. Más acentuadamente nos referimos a la Falsificación Informática, de Instrumentos Públicos y Privados, tema de estudio e interés, que juntamente con el Fraude, Estafa Informática y un derecho consagrado en la Constitución de la República, que es la Privacidad Personal, constituyen infracciones de actualidad en el contexto nacional y local. Y por último, señalo lo tipificado tanto en el Código Penal como en la Ley de Comercio Electrónico sobre los delitos informáticos, y además un análisis de las normas constantes relativas al tema, en los Códigos Penales argentino y español respectivamente. Es menester plasmar una vez terminada la investigación, las Conclusiones las cuales surgen como resultado de este proceso. También las Recomendaciones, que personalmente se pueden contribuir para el mejoramiento y la erradicación del problema planteado, buscando posibles soluciones y/o reformas en el ordenamiento penal. Todos estos temas, se los ha estructurado en esta tesis, en cuatro Capítulos, igual número de Títulos, y dentro de ellos numerales dedicados a los puntos señalados anteriormente.

4. REVISION DE LITERATURA

4.1. CAPITULO I.- INFORMÁTICA.

4. 1.1 CONCEPTO Y NATURALEZA DE LA INFORMÁTICA

Para el Dr. Orlando Solano, Informática, "…es una teoría de la información, que la aborda desde un punto de vista racional y automático, a fin de transformar la información en símbolos y, mediante una serie de mecanismos electrónicos para aplicarla a la mayor cantidad posible de actividades"1.

Según Plein, "la informática es la disciplina que se dedica a estudiar la información y sus componentes, así como la tecnología para manejarla, conservarla y utilizarla de manera eficiente y económica, con miras a facilitar su acceso a otras personas para producir mayores beneficios"2.

Por su parte el Doctor Fernando Jordán Flórez define a la informática como "la ciencia que tiene como objeto propio de su conocimiento la Información; como método, la teoría de sistemas; como instrumento operativo, la computación; como ámbito de desarrollo, la organización; como objetivo, la racionalización, la eficiencia en la acción, a partir del control del proceso de producción y circulación de información; como

1 DÍAZ, Alexander. Derecho Informático. Elementos de la Informática Jurídica. Editorial Leyer. Bogotá Colombia. 2002. Pág.14
2 DÍAZ, Alexander. Derecho Informático. Elementos de la Informática Jurídica. Editorial Leyer. Bogotá Colombia. 2002. Pág.14

misión, la de contribuir a la libertad del ser humano y a la consolidación de la democracia y como valor, el de un bien económico"3.

La Informática, …"la definiríamos como todas las operaciones y procedimientos técnicos, de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias"4.

Informática proviene de información y de automática y sirve para designar el tratamiento y manejo de la información por medio de computadoras"5.

Como criterio propio puedo mencionar que la Informática es la ciencia que estudia todo el proceso de la información, a través de un sistema computacional.

4. 1.2.- DESARROLLO HISTÓRICO DE LA INFORMÁTICA

En cuanto al origen y desarrollo de los ordenadores, de acuerdo a la información obtenida de la Escuela Universitaria de Informática de la

3 Ibídem. Pág.14
4 YÁNEZ, Pablo. Introducción al Estudio del Derecho Informático e Informática Jurídica. ESPOJ. Quito. 1999. Pág.45
5 GUIBOURG, Ricard;Alende, Jorge;Campanella, Elena. Manual de Informática Jurídica. Astrea. Buenos Aires, Argentina.1996. Pág.19

Universidad Politécnica de Madrid, sus antecedentes se deben a los trabajos realizados por "Blaise Pascal (1623-1662) y por Gottfried Leibniz (1646-1716)"6, el primero creó una máquina que era capaz de hacer operaciones de suma y de resta, esto a través de la combinación de una serie de ruedas dentadas, las cuales tenían diez dientes, correspondientes a los números del 9 al 0, este sistema al pasar del nueve al cero, daba lugar a un salto de la rueda continua por el lado izquierdo. Este creación tomó el nombre de Pascalina, posteriormente innovó este dispositivo, al introducir un elemento de memoria mecánica, que permitían acumular resultados parciales, durante las operaciones.

Por su parte Leibniz, mejoró el invento de Pascal, debido a que consiguió que esta máquina desarrolle las cuatro operaciones básicas de la artimética en forma mecánica.

Pero los inicios más progresivos y fundamentales en la esencia misma de la Informática, datan de los trabajos realizados por Hermann Hollerith (1860-1929), miembro de la oficina de censos de Estados Unidos de América, cuyo trabajo consistió en emplear una cinta en la cual se grababa información mediante perforaciones en lugares determinados. Con este dispositivo creado en 1890, fue posible la realización mecánica de operaciones como la clasificación, duplicación y copia de fichas

6 http://www.dma.eui.upm.es/historia_informatica/Flash/principal.htm

perforadas, es decir de los datos contenidos en ellas. Estas máquinas, permitieron efectuar en el tiempo de dos años y medio, el censo de los Estados Unidos de América, que dio como resultado sesenta millones de habitantes.

Siguiendo con los orígenes y desarrollo de la Informática, cabe anotar los trabajos de "Howard H. Aiken (1900-1973), quien desarrolló entre los años de 1939 y 1944 en IBM, un ordenador de nombre MARK I o ASCC (Automatic Secuence Controler Calculator)"7, dicha máquina desde el punto de vista del sistema físico, estaba constituida por un dispositivo eléctrico, el relé (capaz de abrir y cerrar un circuito) y su programación, se llevaba a cabo mediante una cinta perforada, todo esto permitía a este ordenador realizar cualquier operación sin la intervención del hombre, además disponía de una memoria con capacidad de 72 números de 23 cifras decimales, pero era muy lento ya que necesitaba de diez segundos para multiplicar dos números de diez cifras, en cuanto a su peso era de cinco toneladas, incorporaba unos cinco mil relés y ocupaba mucho espacio. Su instalación funcionó desde 1944 hasta 1959. Este fue el primer ordenador de la historia.

7 http://www.dma.eui.upm.es/historia_informatica/Flash/principal.htm

Computadoras de Primera Generación.- Abarca desde el año de 1945 hasta 1958, con ordenadores cuya tecnología era a base de bulbos o tubos de vacío y su programación en lenguaje de máquina. La primera aparece en 1947, la ENIAC (Electronic Numerical Integrator and Calculator), que fue el primer computador totalmente electrónico, diseñado por Jhon Mauchly y Prosper Eckert.

Computadoras de Segunda Generación.- En esta etapa, los computadores ya no usaban válvulas de vacío, sino transistores y se desarrolla a partir de 1951 a 1964, sus ventajas eran: menor consumo de corriente, menor emisión calorífica, ahorro de espacio, se programaban con lenguajes de alto nivel, funcionamiento más fiable y mayor tiempo de duración de sus componentes.

Computadoras de Tercera Generación.- Se desarrollan entre los años de 1965 a 1974, a partir de la invención del circuito integrado o microchip, por parte de Jack St. Claire Kilby y Robert Noyce. Después Ted Hoff inventó el microprocesador, en Intel.

Computadoras de Cuarta Generación.- Desde 1971 a 1988, se caracterizan por las mejoras en la tecnología de las computadoras. La primera, el reemplazo de las memorias con núcleos magnéticos, por las de chip: producto de la microminiaturización de los circuitos electrónicos;

y la segunda, el tamaño reducido del microprocesador de chips, lo que hizo posible la creación de las computadoras personales (PC).

Computadoras de Quinta Generación.- En la actualidad se habla de computadores de quinta generación o "inteligentes" a aquellos ordenadores capaces de reproducir el comportamiento humano en la formulación de decisiones, solución de problemas complejos, como la traducción automática de un lenguaje natural a otro y otras actividades de carácter lógico

- Como una ciencia, la Informática es el "conjunto de técnicas, métodos y máquinas aplicadas al tratamiento automático y lógico de la información"8; y,
- Como actividad científica, "está dirigida a la investigación de los medios que permite el tratamiento y elaboración en forma automática de las informaciones necesarias para el desarrollo de las actividades humanas"9.

Dentro de la clasificación, la Informática se divide en dos campos de estudio: 1) la Informática Fundamental y 2) la Informática Aplicada.

8 YÁNEZ, Pablo. Introducción al Estudio del Derecho Informático e Informática Jurídica. ESPOJ. Quito. 1999. Pág.46
9 Ibídem. Pág.46

1. La Informática Fundamental, es aquella que se encarga del estudio de los fundamentos, sean estos teóricos, técnicos o prácticos, del tratamiento automatizado de datos, y a su vez se subdivide en: a) Informática Técnica; b) Informática Práctica; y, c) Informática Teórica.

2. La Informática Aplicada (Teórica), parte desde que se da una formulación matemática, hasta el estudio actual que constituye el lugar de convergencia de las ciencias informática y matemática.

4.1.3.- SISTEMA DE INFORMACIÓN O TELEMÁTICA

A la telemática, se la concibe como aquella disciplina científica y tecnológica que permite realizar una serie de actividades tecnológicas propias del contexto actual en la evolución de la información, ejemplo "…el poder realizar una llamada telefónica en la cima del monte Elbrus a un abonado en la selva amazónica, enviar un vídeo en 3D por Internet, o hasta recibir imágenes de una sonda que orbita alrededor de un planeta distante"10.

Simon Nora y Alain Minc Electrik, el cual se titula "Informatización de la Sociedad", en el cual se plasmaba una visión precisa a la futura evolución tecnológica. Otros autores manifiestan el origen estadounidense de la

10 VÁSQUEZ, Carlos. Manual de Derecho Informático. Editorial Dijusa. Madrid. 2002. Pág.26

telemática, el término *compunication*, más conocido y utilizado como *Computer and Communications*. La diferencia radica básicamente por responder a contextos muy diferentes; la aclaración de esta distinción, es situarse en la respectiva época, por una parte Francia, ponía énfasis en las telecomunicaciones, motor de su transformación social (1976), en tanto que Estados Unidos vivía su gran evolución informática. Ahora bien, la comunicación apunta a un modelo relevante en los sistemas informáticos; la telemática se refiere a poner énfasis en la telecomunicación. Cada una apunta a un destino diferente al parecer, mas la realidad nota que han convergido en un solo cuerpo, una sola disciplina científica y tecnológica, abarcando al mundo informático. Esta es la telemática o sistema de información.

Una vez que hemos hecho referencia a la telemática, ahora bien señalo lo concerniente al sistema de información, materia que se concatena con la anterior, proporcionado mayor claridad a este capítulo de estudio.

Sistema de información es "un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su posterior uso, generados para cubrir una necesidad"11.

11 VÁSQUEZ, Carlos. Manual de Derecho Informático. Editorial Dijusa. Madrid. 2002. Pág.36

Los elementos de este sistema, forman una cadena o enlace dirigidos a la obtención de la información óptima, en el sitio lugar requerido.

En síntesis la telemática o sistema de información, se presenta como aquel concepto explicativo del trabajo organizado de los especialistas en las materias informática, electrónica y de telecomunicaciones, en su misión del desarrollo, almacenamiento y procesamiento de datos, así como la generación de herramientas de gestión y control de procesos, basados en estadísticas y procesamiento de información.

4.1.4.- INFORMÁTICA JURÍDICA

Dentro de la obra Elementos de la Informática Jurídica, el Dr. Fernando Jordán Flórez, define a la Informática Jurídica como "la utilización de los diferentes conceptos, categorías, métodos y técnicas propios de la Informática en el ámbito de lo jurídico"12.

El Dr. Héctor Peñaranda nos dice que la Informática Jurídica es "la ciencia que estudia la utilización de aparatos o elementos físicos electrónicos, como la computadora, en el derecho; es decir, la ayuda que este uso presta al desarrollo y aplicación del derecho"13.

12 DÍAZ, Alexander. Derecho Informático. Elementos de la Informática Jurídica. Editorial Leyer.Bogotá Colombia. 2002. Pág.14
13 Ibídem. Pág.15

Para el Dr. Marcelo Bauzá Reilly, Secretario General de la Federación Iberoamericana de Asociaciones de Derecho e Informática, la Informática Jurídica es "el tratamiento lógico y automático de la información jurídica, en tanto soporte del conocimiento y la comunicación humana"14.

Según el jurista español Antonio Enrique Pérez Luño, define a la informática jurídica como la técnica que tiene por finalidad almacenar, ordenar, procesar y entregar según criterio lógico y científico, todos los datos jurídicos necesarios para documentar o proponer la solución al problema de que se trate, mediante el estudio del tratamiento automatizado de las fuentes del conocimiento jurídico y de los medios instrumentales con que se gestiona el Derecho.

El autor de la obra Derecho Informático, Julio Núñez Ponce, dice que Informática Jurídica es la aplicación de la Informática del Derecho, permitiendo que exista una base de datos computarizada, que automatice la gestión de un estudio, secretaría de Juzgado, Notaría, etc, y sistematice el conocimiento jurídico a través de la inteligencia artificial.

La Informática Jurídica es "…la técnica interdisciplinaria que tiene por objeto el estudio e investigación de los conocimientos de la Informática

14 Ibídem. Pág.16

general, aplicable a la recuperación de información jurídica, así como la elaboración y aprovechamiento de los instrumentos de análisis y tratamiento de información jurídica necesarios para lograr dicha recuperación. En sentido general, la Informática Jurídica es el conjunto de aplicaciones de la informática en el ámbito del Derecho"15.

Para Antonio Pérez Luño, autor del Manual de Informática y Derecho, la Informática Jurídica estudia el tratamiento automatizado de: las fuentes de conocimiento jurídico, a través de los sistemas de documentación legislativa, jurisprudencial y doctrinal; las fuentes de producción jurídica, a través de la elaboración informática de los valores lógico formales que concurren en el proceso legislativo y en la decisión judicial; y los procesos de organización de la infraestructura o medios instrumentales con los que se gestiona el Derecho.

En otra definición dada por la doctrina se manifiesta que "…Informática Jurídica es todo procedimiento electrónico, telemático o en general científico de tratamiento de la información que permite la actualización, mejora, desarrollo de los sistemas y procesos en materia jurídica, participando además en la solución de sus problemas"16.

15 TÉLLEZ, Julio. Derecho Informático. Tercera Edición. MacGrawHill. México.2003. Pág.19
16 YÁNEZ, Pablo. Introducción al Estudio del Derecho Informático e Informática Jurídica. ESPOJ. Quito. 1999. Pág.79

La Informática Jurídica, la podemos definir como aquella ciencia, que estudia la aplicación de la Informática en el ámbito de lo jurídico, entendiendo esto, como la utilización de procedimientos sistematizados y automatizados, que a través de un computador, permite dar soluciones a problemas o situaciones jurídicas.

4.1.5.- DERECHO INFORMÁTICO

La doctrina nos trae varias definiciones a continuación:

La definición de Derecho Informático, para el Dr. Héctor Peñaranda, señala que: "es el conjunto de normas, aplicaciones, procesos, relaciones jurídicas que surgen como consecuencia de la aplicación y desarrollo de la informática"17.

El tratadista Dr. Marcelo Bauzá Reilly, define al Derecho Informático como: "el conocimiento de problemas jurídicos producidos por la Informática"18.

Otra definición dada por la doctrina señala que el Derecho Informático, es "…el conjunto de normas o leyes que rigen las relaciones entre las

17 DÍAZ, Alexander. Derecho Informático. Elementos de la Informática Jurídica. Editorial Leyer. Bogotá Colombia. 2002. Pág.16

18 Ibídem. Pág.16

personas creadas mediante el uso de cualquier medio tecnológico existente o que se llegase a crear, que transmita y procese información"19.

El Derecho Informático se lo define como "el conjunto de leyes, normas y principios aplicables a los hechos y actos derivados de la Informática. Es decir, es un conjunto de leyes en cuanto que, si bien escasos, existen varios ordenamientos jurídicos nacionales e internacionales con alusión específica al fenómeno informático"20.

"Derecho Informático regula las diversas relaciones jurídicas, políticas, sociales y económicas que se producen a raíz del uso y del abuso de la informática, y conjuntamente de las telecomunicaciones"21.

Y por último el Derecho Informático es "la aplicación del Derecho a la Informática permitiendo que se adopten o creen soluciones jurídicas a los problemas que surgen en torno al fenómeno informático"22.

Después de observar cada una de las definiciones propuestas, me permito manifestar, que el Derecho Informático es el conjunto de normas preceptos y principios jurídicos que regulan las

19 YÁNEZ, Pablo. Introducción al Estudio del Derecho Informático e Informática Jurídica. ESPOJ. Quito. 1999. Pág.162
20 TÉLLEZ, Julio. Derecho Informático. Tercera Edición. MacGrawHill. México.2003. Pág.21
21 JIJENA, Renato. Chile, la Protección Penal de la Intimidas y el Delito Informático. Editorial Jurídica de Chile. Santiago de Chile.1992.Pág.19,20
22 YÁNEZ, Pablo. Introducción al Estudio del Derecho Informático e Informática Jurídica. ESPOJ. Quito. 1999. Pág.161

correspondientes relaciones y los efectos que se producen entre los seres humanos dentro de la Informática.

Es el Derecho especializado en la Informática, que ha nacido por la necesidad de contar con una normativa que permita regular todas y cada una de las acciones y consecuencias que ocurren dentro del campo del desarrollo y evolución de la Informática. Asimismo el Derecho Informático está integrado por "las sentencias de los Tribunales sobre materias informáticas y las proposiciones normativas, es decir, los razonamientos teóricos del Derecho que tiene por objeto analizar, interpretar, exponer, sistematizar o criticar el sector normativo que disciplina la informática y la telemática"23.

Es así que surge el Derecho Informático como una rama del Derecho que permite otorgar las soluciones jurídicas adecuadas a los problemas originados por el uso de las tecnologías, en las diversas actividades del ser humano.

Y con el uso de estas nuevas tecnologías en el campo del Derecho, los abogados, juristas, jueces y en general todas las personas inmersas en los temas jurídicos, no podemos alejarnos de la realidad que representa

23 Ibídem. Pág.250

las nuevas relaciones basadas en microchips, circuitos, ordenadores, satélites y en el mundo de la informática y la computación. Ejemplo de esto, representa el domicilio que hoy tanto las empresas, las instituciones de la administración pública, así como nosotros mismos, publican e indican un domicilio electrónico (correo electrónico) o páginas web, para recibir notificaciones, noticias, mensajes, etc.

"La importancia de la relación entre Informática y Derecho también acude en otro entorno distinto al de los efectos creados por las nuevas relaciones jurídicas originadas por el uso de nuevas tecnologías y es precisamente la adaptación de esas nuevas tecnologías al mundo de lo jurídico"24.

4.2 CAPITULO II.- DELITOS INFORMÁTICOS.

4. 2.1 DELITO

Primeramente definiremos al Delito, como toda acción típica, antijurídica, culpable y punible. Es una acción, porque se genera de un acto del ser humano. Típica, porque la acción u omisión, debe estar claramente definida por la ley penal, para que ésta pueda ser penada. Antijurídica, pues la acción debe estar totalmente en oposición y contraria a la normativa penal. Culpable, es decir que el delito debe estar revestido de

24 YÁNEZ, Pablo. Introducción al Estudio del Derecho Informático e Informática Jurídica. ESPOJ. Quito. 1999. Pág.59,60

dolo, que es la intención de hacer daño, y de culpa, que es la falta de cuidado o negligencia de quien comete el delito. Con estos dos caracteres, nos posicionamos frente a la culpabilidad de la conducta del ser humano. Punible, que la acción realizada está tipificada y sancionada con una pena determinada.

El jurisconsulto y profesor italiano Francisco Carrara, (Lucca, 1805 – 1888), nos da una definición clara acerca del delito, como es, la infracción de la ley del estado, promulgada para proteger la seguridad de los ciudadanos, y que resulta de un acto externo del hombre, positivo o negativo, moralmente imputable y socialmente dañoso.

4.2.2 DELITO INFORMÁTICO

El Dr. Solano, define al Delito Informático desde dos conceptos: uno restringido y otro amplio, el primero "tiene como aquel hecho en el que independientemente del perjuicio que puede causarse a otros bienes jurídicamente tutelados y que eventualmente puedan concurrir en forma real o ideal, se atacan elementos puramente informáticos. Tales serán los casos del uso indebido del software, apropiación indebida de datos, interferencias en sistemas de datos ajenos"25, y en el segundo

25 DÍAZ, Alexander. Derecho Informático. Elementos de la Informática Jurídica. Editorial Leyer. Bogotá Colombia. 2002. Pág.155

manifiesta que "es la acción típica, antijurídica y culpable para cuya consumación se utiliza o se afecta a una computadora o sus accesorios"26.

El tratadista Téllez Valdés manifiesta que "no es labor fácil dar un concepto sobre delitos informáticos, en razón de que su misma denominación alude a una situación muy especial, que para hablar de delitos en el sentido de acciones típicas, es decir, tipificadas o contempladas en textos jurídicos penales, se requiere que la expresión "delitos informáticos" esté consignada en los Códigos Penales, lo cual en nuestro país, al igual que en otros muchos no ha sido objeto de tipificación aún"2746.

El Delito Informático es"…toda conducta típica, antijurídica y culpable realizada a través del hardware y/o software o contra el computador y/o programa siempre en perjuicio de una persona"28.

El Dr. Claudio Líbano Manzur describe al Delito Informático como "aquellas acciones u omisiones típicas, antijurídicas y dolosas, trátese de hechos aislados o de una serie de ellos, cometidos contra personas

26 DÍAZ, Alexander. Derecho Informático. Elementos de la Informática Jurídica. Editorial Leyer. Bogotá Colombia. 2002. Pág.155

27 MÁRQUEZ, Carlos. El Delito Informático. La Información y la Comunicación en la Esfera Penal. Editorial Leyer. Bogotá Colombia. 2002.Pág.84

28 OCAMPO, Marcela, HERNÁNDEZ Boris. Derecho e Informática. Pontificia Universidad Javeriana. Bogotá. 1987. Pág.234

naturales o jurídicas, realizadas en uso de un sistema de tratamiento de la información y destinadas a producir un perjuicio en la víctima a través de atentados a la sana técnica informática, lo cual…, producirá lesiones a distintos calores jurídicos, reportándose, muchas veces, un beneficio ilícito en el agente, sea o no de carácter patrimonial, actúe con o sin ánimo de lucro"29.

Esta definición hace referencia al sujeto activo, sujeto pasivo y al bien jurídico protegido que es lesionado por el agente realizador de este ilícito, en donde a través del uso de un sistema informático, se enfoca en causar un perjuicio moral, económico, social en quienes son víctimas.

Rodolfo Herrera Bravo, entiende por Delito Informático a "la acción típica, antijurídica y dolosa cometida mediante el uso normal de la informática, contra el soporte lógico o software de un sistema de tratamiento automatizado de la información"30.

Características de los Delitos Informáticos.- Entre las características principales de los Delitos Informáticos, se puede señalar las siguientes:

a) Son cometidos a través de un ordenador;

b) Pueden ocupar un programa informático para cometer el ilícito;

29 DÍAZ, Alexander. Derecho Informático. Elementos de la Informática Jurídica. Editorial Leyer. Bogotá Colombia. 2002. Pág.155

30 MÁRQUEZ, Carlos. El Delito Informático. La Información y la Comunicación en la Esfera Penal. Editorial Leyer. Bogotá Colombia. 2002.Pág.88

c) Son rápidos en su cometimiento y fáciles de ocultar;

d) Difíciles al momento de identificar a su autor;

e) Fáciles para borrar las pruebas de su ejecución;

f) Generan pérdidas económicas;

g) Son pocos o casi nulos en ser denunciados;

h) Son de carácter doloso, por la malicia e intencionalidad con que se cometen; y,

i) Son prolíferos, de acuerdo a las estadísticas y casos que cada día se presentan en un mayor grado.

Las personas que cometen esta clase de delitos, poseen características propias, que los diferencia de la delincuencia común, debido a su alto grado de preparación, a saber:

a) Son personas jóvenes;

b) Poseen suficientes conocimientos en el área de la Informática.

c) Ocupan lugares estratégicos en su trabajo, en donde tienen acceso a información confidencial, archivos o bases de datos.

d) Son personas "inteligentes, imaginativas, activas;

e) Se debe claramente identificar al delincuente informático, pues no es lo mismo el joven que entra a un sistema informático por curiosidad, por

investigar, que el empleado de una institución financiera que desvía los fondos de las cuentas de sus clientes.

En suma, se puede considerar a los delincuentes informáticos como personas con amplios conocimientos de Informática, capaces de causar un funcionamiento inapropiado de sistemas informáticos.

4.2.3 DELINCUENCIA INFORMÁTICA

En el mundo actual, se habla y se entiende por delincuentes, independientemente y en sus diversas esferas, a las personas quienes cometen ilícitos, es decir que no respetan las leyes que rigen en la sociedad, violándolas cada vez con mayor frecuencia. Y al hablar de delincuencia, se refiere a grupos de personas que cometen delitos, cualquiera que estos sean, y es así que se ha llegado a formar una sociedad en donde silenciosamente impera la delincuencia informática, que al respecto, se refiere a delincuentes quienes cometen delitos mediante la Informática o las tecnologías de la información. Una de las víctimas de la delincuencia informática fue Lourdes Abarca quien asegura haber sido estafada en el instante en que intentó comprar una computadora vía internet: “yo quería adquirir una computadora, una laptop y a mí me habían dicho unos amigos que habían comprado por internet sin ningún problema en la páginas de compra y venta, y entonces

me habían dicho que no tenía ningún problema, que era muy seguro y todo, entonces intenté, me metí a las páginas y quedé de acuerdo con un señor , una laptop era 1600 y pico , no me acuerdo mucho, espere varios días y al momento de recibir la máquina ya pasó la semana y el señor no me contestó más, me quejé con la página y todo, y así fue , me estafó"31.

Los delincuentes informáticos, también son conocidos como crackers, personas que modifican el funcionamiento normal tanto del hardware como del software de un sistema informático, con intenciones propias de causar daño, o a su vez al ser contratados por terceras personas, ejecutan tareas encaminadas a perjudicar a sectores que contienen informaciones trascendentales o importantes, siempre buscando un beneficio a cambio del perjuicio de otros, como es la falsificación de tarjetas de crédito, todo esto por obtener réditos económicos.

En fin, podemos catalogar a la delincuencia informática como un grupo de personas, con conocimientos suficientes de Informática, capaces de causar un funcionamiento anormal de sistemas informáticos. Existiendo terceras personas, sin mucho conocimiento de los delitos informáticos, pero que actúan como cómplices, al momento de dar por ejemplo, claves de tarjetas de crédito, clonar tarjetas o el libre acceso a datos,

31 Programa Día a Día. Teleamazonas.- Domingo 13 de junio de 2010

archivos, archivos o informaciones. En el caso de producirse un delito informático, surge la necesaria investigación de ubicar a las personas que ingresaron datos, las personas quienes tuvieron el acceso libre a esos sistemas, todo cuanto implica el procesamiento de datos, incluyendo a programadores, operadores y demás usuarios que libremente elaboraron los programas de acceso y función del sistema informático.

4.2.4 SUJETOS

4.2.4.1. SUJETO ACTIVO

Según el Diccionario Jurídico Elemental del autor Guillermo Cabanellas (pág. 374), el sujeto activo del delito es "el autor, cómplice o encubridor; el delincuente en general". Por consiguiente podemos aseverar que el sujeto activo es el delincuente que realiza o ejecuta el delito informático, y siendo más preciso es el autor, cómplice o encubridor que comete la falsificación informática. El nivel de aptitud del delincuente informático es tema de controversia, ya que para algunos, este nivel no es un indicador de delincuencia informática, en tanto que para otros, "los delincuentes informáticos son personas listas, decididas, motivadas y dispuestas a aceptar un reto tecnológico, características que pudieran encontrarse en un empleado del sector de procesamiento de datos", sin que por este motivo se configure el cometimiento de un delito, una falsificación informática.

En nuestro país estos sujetos activos han logrado vulnerar páginas web de bancos, de empresas, instituciones públicas como las prefecturas y aún hasta la misma Asamblea Nacional ha sido blanco de los delitos informáticos y la falsificación informática.

4.2.4.2 SUJETO PASIVO

Al respecto el Diccionario Jurídico de Cabanellas en la página 296, señala que el sujeto pasivo es el "que recibe la acción del agente, y no coopera en ella".

Otra definición señala que el sujeto pasivo "es la persona natural o jurídica titular del bien jurídico que el legislador protege y sobre la cual recae la actividad típica del sujeto activo32".

A estas definiciones es necesario manifestar que la acción (que recibe) o (sobre la cual recae) la actividad típica, es el delito informático (falsificación informática), con lo cual asevero que el sujeto pasivo es aquella persona natural o jurídica sobre la cual se perpetra el delito informático o la falsificación informática, emanada o realizada por el sujeto pasivo.

Ampliando esta definición, se distingue que el sujeto pasivo del delito es

32 ACURIO, Santiago. Ruptura por la legalidad. F&R Gráficas. Quito Ecuador. 2001. Pág.309

el ente o la víctima sobre la cual recae la conducta de acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos y la falsificación informática, las víctimas pueden ser cualquier individuo o persona natural, así también personas jurídicas como instituciones bancarias, gobiernos, etc, mismos que usan sistemas automatizados de información.

4.2.5.- BIEN JURÍDICO PROTEGIDO

El Diccionario Jurídico de Cabanellas señala en cuanto al bien jurídico, "aunque cabe hablar de un bien mueble, inmueble o incorporal, el tecnicismo prefiere emplear el plural (bienes) para referirse a cuanto puede constituir objeto de un patrimonio".

Roxin Claus, define al bien jurídico como "las circunstancias dadas o finalidades que son útiles para el individuo y su libre desarrollo en el marco de un sistema global estructurado sobre la base de esa concepción de los fines o para el funcionamiento del propio sistema"33.

Carlos Márquez, manifiesta que "los bienes jurídicos son todos aquellos intereses privados que el Estado ha expropiado y tomado como suyos y que, debido a su puesto papel de benefactor, ha de garantizar"34.

33 MÁRQUEZ, Carlos. El Delito Informático. La Información y la Comunicación en la Esfera Penal. Editorial Leyer. Bogotá Colombia. 2002. Pág.97
34 Ibídem. Pág.97

“El patrimonio, en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar; La reserva, la intimidad y confidencialidad de los datos, en el caso de las agresiones informáticas a la esfera de la intimidad en forma general, especialmente en el caso de los bancos de datos; La seguridad o fiabilidad del tráfico jurídico y probatorio, en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos; El derecho de propiedad, en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los daños y el llamado terrorismo informático”88.

En el caso de los delitos informáticos, los bienes jurídicos protegidos podrían ser diversos en atención hacia aquellos a los que está dirigido el acto lesivo, valiéndose a través o por medio del ordenador que permite el acceso a información que se procesa en un sistema informático.

4.3 CAPITULO III.- FALSIFICACIÓN.

4.3.1 FALSIFICACIÓN INFORMÁTICA

El Diccionario de la Real Academia Española de la Lengua, define a la falsificación como “acción o efecto de falsificar; falsificar en cambio es

falsear, adulterar o contrahacer. Proviene del Latín falsificare, de falsus, falso".

"La falsedad recae sobre la materialidad del documento, sobre sus signos de autenticidad incluidos los que forma parte de su contenido, ya sea porque se los imita, creándolos, o se los modifica, alterando su veracidad"35.

Siendo el término Informática, como ya quedó señalado la información automática, la falsificación informática, entonces sería una falsedad, algo contrario a la verdad vía informática o computarizada.

Para efectuar una falsificación electrónica o informática, el sujeto activo se vale de ordenadores, impresoras, scanner, copiadoras, etc. para elaborar documentos, copiando las mismas formas, estilos de letras, logotipos, y demás adulteraciones.

Por su parte, la doctrina jurídica, asevera que la Falsificación Informática, sucede o es "cuando se alteran datos de documentos que se encuentran almacenados en forma computarizada. Pueden falsificarse o adulterarse también micro formas, micro duplicados y microcopias; esto

35 MANERA, Alberto E. Falsedades Documentales por Computadora. Ediciones La Rocca. Falsificación de documentos. Delito Informático. Buenos Aires, Argentina.2006.Pág.17

puede llevarse a cabo en el proceso de copiado en cualquier otro momento"36.

Cabanellas afirma que la falsificación en general es la "adulteración, corrupción, cambio o imitación para perjudicar a otro u obtener ilícito provecho; ya sea en la escritura, en la moneda, en productos químicos, industriales o mercantiles, etc. Delito de falsedad cometido en documento público o privado…".

En este sentido, puedo concluir en que la Falsificación Informática, es la adulteración o cambio en el contenido de un instrumento sea éste público o privado, que posee información procesada a través de un sistema informático.

Como características de la falsificación informática, señalo las siguientes:

a) Es doloso, en vista que en el sujeto activo hay la voluntad tácita de delinquir, es decir causar un daño, esto con el uso de de un computador para modificar o alterar los instrumentos, mensajes de datos o cualquier tipo de información.

36 DÍAZ, Alexander. Derecho Informático. Elementos de la Informática Jurídica. Editorial Leyer. Bogotá Colombia. 2002. Pág.159

b) Es un delito de cuello blanco, anteriormente se decía que para el cometimiento de este delito, se requiere que determinadas personas cuenten con un nivel alto de preparación y conocimientos específicos en la materia informática, lo cual hace suponer que se realicen en un nivel alto cultural y económicamente, mas ahora vemos como cualquier joven con relativos conocimientos, se puede convertir en un delincuente informático, esto debido al fácil acceso a la tecnología.

c) Son ejecutables en un momento propicio, en vista de su ejecución, el hecho de correr el riesgo implicado en una falsificación, se produce cuando hay un alto beneficio o ganancia.

d) Son consumados rápidamente, son acciones que las realizan en pocos minutos o segundos, puesto que se cuenta con la tecnología y la habilidad suficiente.

e) Es un delito que genera grandes pérdidas económicas, refiero a las falsificaciones de tarjetas de crédito y débito.

f) Es un delito en constante crecimiento y asimismo poco denunciado.

4.3.2 FALSIFICACIÓN INFORMÁTICA DE INSTRUMENTOS PÚBLICOS

El Código de Procedimiento Civil ecuatoriano señala en su Art. 164.- "Instrumento público o auténtico es el autorizado con las solemnidades legales por el competente empleado. Si fuere otorgado ante notario e incorporado en un protocolo o registro público, se llamará escritura pública.

Se consideran también instrumentos públicos los mensajes de datos otorgados, conferidos, autorizados o expedidos por y ante autoridad competente y firmados electrónicamente".

El Art. 165 del C. P. C. señala que: "Hacen fe y constituyen prueba todos los instrumentos públicos, o sea todos los instrumentos autorizados en debida forma por las personas encargadas de los asuntos correspondientes a su cargo o empleo, como los diplomas, decretos, mandatos, edictos, provisiones, requisitorias, exhortos u otras providencias expedidas por autoridad competente; las certificaciones, copias o testimonios de una actuación o procedimiento gubernativo o judicial, dados por el secretario respectivo, con decreto superior, y los escritos en que se exponen los actos ejecutados o los convenios celebrados ante notario, con arreglo a la ley; los asientos de los libros y otras actuaciones de los funcionarios y empleados del Estado de cualquiera otra institución del sector público; los asientos de los libros y

registros parroquiales, los libros y registros de los tenientes políticos y de otras personas facultadas por las leyes.

El Art. 178 del Código de Procedimiento Civil, dispone "Es instrumento falso es el que contiene alguna suposición fraudulenta en perjuicio de tercero, por haberse contrahecho la escritura o la suscripción de alguno de los que se supone que la otorgaron, o de los testigos o del notario; por haberse suprimido, alterado o añadido algunas cláusulas o palabras en el cuerpo del instrumento, después de otorgado; y en caso de que hubiere anticipado o postergado la fecha del otorgamiento".

Estas definiciones de la normativa civil, cubren y abarcan todo los ámbitos referentes al instrumento público sobresaliendo lo esencial, que debe ser otorgado ante una autoridad competente, dándole valor legal a su existencia, hace una clasificación detallada de cada uno de los que se consideran instrumentos públicos, y además de dejar en claro que la adulteración, supresión o añadidura en un instrumento público es lo concerniente a la falsificación y en nuestro ámbito a la falsificación informática.

La falsificación informática de instrumentos públicos, podría decir que es un delito informático en el cual se altera o modifica el contenido de un instrumento o documento público, mediante el uso de la informática.

En nuestro país, ha sido muy difundido el cometimiento de este delito, principalmente por funcionarios públicos encargados del otorgamiento de instrumentos públicos. El 8 de diciembre de 2010, el diario Expreso, trae la noticia "Policía desarticula banda que tramitaba cédulas para cubano". Funcionarios del Registro Civil, estarían implicados. Agentes de la Brigada de Misceláneos de la Policía Judicial de Pichincha desarticularon una supuesta banda de tramitadores de cédulas de ciudadanía para cubanos que operaba en distintas ciudades del país. Tras varios meses de investigación, fueron detenidos: Gissela Raquel Cabezas Gutiérrez, Leder Jhonatan Espinoza Estupiñán, Carmen Luisa León Valladares, Rodolfo Elías Astudillo y Joffre Mauricio Barragán Paz, funcionarios de las oficinas del Registro Civil en Puerto Quito, Esmeraldas, Quinindé y Guayaquil, quienes estarían implicados en la entrega fraudulenta de cédulas a los extranjeros. La denuncia presentada por un ciudadano cubano, quien aseguró que se lo pretendía estafar con 3.750 dólares cuando intentó legalizar sus documentos, levantó las sospechas de las autoridades de que estaría operando una banda de falsificadores. Según la Policía, el tramitador tenía su oficina en el sector de Santa Prisca, desde donde realizaba las diligencias de naturalización de cubanos. El individuo, supuestamente solicitó documentos personales, fotos y dos hojas en blanco firmadas por el extranjero para realizar los trámites. Luego le entregaron una cédula como ciudadano ecuatoriano y cuatro

días después el pasaporte. Pero al solicitar la carta de naturalización el tramitador le explicó que no existía porque el matrimonio no estaba inscrito en los libros y que los otros documentos entregados eran legales. Fue entonces cuando el extranjero decidió denunciar el caso a las autoridades, cuyas investigaciones continúan para determinar si hay más personas implicadas en el delito de falsificación".

Como este caso, varios han ido suscitándose años atrás, por parte de propios funcionarios de entidades públicas, en este caso, de los Registros Civiles del país, sin un control de las autoridades respectivas, sin embargo de ser un problema social, muchas de las veces cuentan con el silencio de quienes conocen estos delitos y no los denuncian, o a su vez han caído en complicidad con la gente que comete este ilícito, ya sea por ahorrarse tiempo en sacar un documento o para generar un beneficio económico a través de lo ilegal.

En el diario El Universo del lunes 07 de julio del 2008, en el cual se manifiesta que: "Alexandra Rodríguez Jiménez, quien fue alertada el pasado 28 de mayo mediante una llamada telefónica de un empleado de Comandato. "Llamaron a mi casa y le indicaron a mi esposo que me acercara a la oficina del local comercial, en la Alborada, para retirar la tarjeta de crédito que según supuestamente solicité", dijo la perjudicada. "Mi esposo sorprendido les aclaró que yo no solicité ninguna tarjeta,

pero el empleado le replicó que en el almacén consta que adquirí unos electrodomésticos el pasado 8 de mayo, por 1.800 dólares", agregó. Ante esto, Carlos Benavides, gerente de la Multitienda de Comandato, expresó que en el último mes se detectaron 10 casos de estafa, donde suplantaban la identidad de personas con cédulas falsa, a las que le colocaban las fotos y firmas de quienes aspiraban ilegalmente a el crédito. "La cédula es original, pero está trabajada", dijo Benavides, tras agregar que no se explica cómo los estafadores consiguen los documentos. En esta misma casa comercial María Álvarez Intriago, quien es odontóloga, fue también víctima de la suplantación de identidad. "A mi hija le falsificaron la cédula y a su nombre sacaron un crédito para adquirir electrodomésticos por un monto de 2.000 dólares", dijo Hilario Álvarez, padre de la perjudicada. El gerente de la multitienda expresó que entre abril y mayo se detectaron al menos 50 casos en los que intentaron suplantar las identidades de otras personas, las que fueron descubiertas a tiempo, antes de otorgar los créditos y entregar los electrodomésticos. "Tenemos un departamento de crédito capacitado y antes de otorgar las tarjetas verificamos direcciones, así evitamos las estafas, que no solo perjudican a la persona suplantada sino a la casa comercial que asume el monto perdido", añadió. Otro caso similar es el de Carmen Pérez Chacón, quien pasó una pesadilla cuando la llamaron de una entidad bancaria para decirle que tenía que llevar un certificado del

Consejo Nacional de Control de Sustancias Estupefacientes y Psicotrópicas (Consep) para abrir una cuenta bancaria que solicitó tiempo atrás. "Alguien suplantó mi identidad y estuve en problemas de droga, tuve que tramitar en el Consep el certificado y comprobar que no era mi identidad", dijo Pérez. Asimismo, Danilo Murtinho presentó una denuncia en el Ministerio Público por falsificación de cédula y suplantación de identidad. A su nombre sacaron servicios de televisión pagada, telefónicos y crédito de electrodomésticos en las casas comerciales Japón y Comandato…".

4.3.3 FALSIFICACIÓN INFORMÁTICA DE INSTRUMENTOS PRIVADOS – TARJETAS DE CRÉDITO.

Es fácil predecir que los documentos tradicionales serán sustituidos por los instrumentos electrónicos, caracterizados en ser leídos o conocidos por el hombre, gracias a un sistema o dispositivos informatizados, traductores de su contenido digital. Esto lo observamos en el caso de las tarjetas magnéticas, construidas para el uso de terminales de un sistema, las tarjetas de crédito utilizadas para acceder a cuentas bancarias, vía lectura de los respectivos cajeros automáticos.

El artículo 191 del Código de Procedimiento Civil señala que "Instrumento privado es el escrito hecho por personas particulares, sin

intervención de notario ni de otra persona legalmente autorizada, o por personas públicas en actos que no son de su oficio"37. El Art. 192 expresa "Se pueden extender en escritura privada los actos o contratos en que no es necesaria la solemnidad del instrumento público"38. En el 193 indica "Son instrumentos privados:

1.- Los vales simples y las cartas;

2.- Las partidas de entrada y las de gasto diario;

3.- Los libros administrativos y los de caja;

4.- Las cuentas extrajudiciales;

5.- Los inventarios, tasaciones, presupuestos extrajudiciales y asientos privados; y,

6.- Los documentos a que se refieren los Arts. 192 y 194"39. Y por último el Art. 194 señala.- "El instrumento privado en que una persona se obliga a dar, hacer o no hacer alguna cosa, o en que confiesa haberla recibido o estar satisfecha de alguna obligación…"40.

En el código indicado, no se hace mención acerca de los instrumentos privados como las tarjetas de crédito, cosa que debería constar, sin duda no es menos cierto que estos instrumentos son muy conocidos y

37 Ediciones Legales.- Código de Procedimiento Civil.- Art. 191
38 Ediciones Legales.- Código de Procedimiento Civil.- Art. 192
39 Ediciones Legales.- Código de Procedimiento Civil.- Art. 193
40 Ediciones Legales.- Código de Procedimiento Civil.- Art. 194

portados por la mayoría de gente, sabiendo que es un documento real, útil y necesario para generar la relación bancaria y comercial a diario.

Los tratadistas Carlos Creus y Jorge Buompadre, en su obra "Falsificación de documentos en general", manifiestan que instrumento privado es "todo el que, sin presentar las características precedentemente consignadas (instrumento público), manifiesta un tenor asignable a un sujeto determinado, con efectos jurídicos.

La falsificación informática de un instrumento privado, es por consiguiente aquel delito consistente en la adulteración, cambio, modificación realizada en el contenido de un instrumento privado, utilizando a la informática como un medio u objeto para tales fines.

Este delito, atenta contra la seguridad de las bases de datos mercantiles del comercio electrónico, en las cuales se accede a informaciones sobre los clientes de una institución crediticia o bancaria, específicamente dirigida a la clonación y falsificación de tarjetas de crédito y de débito.

Los riesgos frecuentes relacionados con el acceso a un sistema de información, son los relativos a la falsificación de tarjetas o a la sustracción de claves y al peligro que corre el propio usuario si no

custodia adecuadamente su tarjeta o no guarda secreto acerca de su clave.

Instrumento privado es "todo el que, sin presentar las características precedentemente consignadas (instrumento público), manifiesta un tenor asignable a un sujeto determinado, con efectos jurídicos"41.

La falsificación informática de un instrumento privado, es por consiguiente aquel delito consistente en la adulteración, cambio, modificación realizada en el contenido de un instrumento privado, utilizando a la informática como un medio u objeto para tales fines.

Según la doctrina, un documento electrónico o informático es "un conjunto de impulsos eléctricos que recaen en un soporte de computadora, y que sometidos a un adecuado proceso, permiten su traducción a lenguaje natural a través de una pantalla o una impresora"42.

Los antecedentes de los instrumentos privados, hablando de las tarjetas de crédito y/o débito, se ubican en la evolución histórica de la moneda,

41 CREUS, Carlos, BUOMPADRE, Jorge. Falsificación de documentos en general. ASTREA. Argentina. 1986. Pág.45
42 TÉLLEZ, Julio. Derecho Informático. Tercera Edición. MacGrawHill. México.2003. Pág.247

empezando por el trueque, pasando por el dinero físico, hasta llegar a su abstracción y desmaterialización como lo conforman los pagarés, letra de cambio, cheques, etc, y ahora en día se ha llegado a una sociedad dentro de la cual, los bienes y servicios se los adquiere sin contar con dinero en efectivo, basta la sola presencia del dinero plástico, a decir de las tarjetas.

La tarjeta de crédito, "consiste en el documento mercantil, instrumental electrónico, mediante el que su titular tiene acceso a una línea de crédito asociada a una relación previamente acordada"43.

Las tarjetas de crédito/débito, "son documentos mercantiles, electrónicos, cuyo soporte constituye un plástico rígido, permitiendo identificar a los sujetos: acreedor y deudor de un crédito previamente acordado, permitiendo a su titular adquirir bienes o servicios o disponer de dinero en efectivo"44.

Las características de la Tarjeta de Crédito son las siguientes:

a) Es un instrumento mercantil electrónico,

b) su soporte y base es de plástico rígido,

43 YÁNEZ, Pablo. Introducción al Estudio del Derecho Informático e Informática Jurídica. ESPOJ. Quito. 1999. Pág.206

44 Ibídem. Pág.207

c) contiene una banda magnética, donde se almacena su información

d) está basado en una relación de crédito, establecida previamente,

e) constituye una obligación de pago o deuda a su titular y genera un derecho de cobro o acreedor a su emisor; y,

f) su uso está dirigido a la compra de bienes y servicios, y al pago diferido.

Su característica principal se resume en que constituye un medio de pago.

Dentro de las características de las tarjetas de débito, a más de las tres primeras enunciadas anteriormente, señalo las siguientes:

a) Sirve para extraer información de cuentas bancarias del titular, a través de los cajeros automáticos,

b) puede ser utilizada como instrumento de garantía; y

c) su función se destina a sacar en efectivo, si por supuesto el cliente tiene dinero en su cuenta, o para hacer transacciones como pagos, consultas y transferencias.

Estos instrumentos en general, son creados con la intervención de todo un sistema informático (la combinación de periféricos de entrada y salida de un ordenador), y por consiguiente su función y uso con este sistema.

Dentro de nuestro país, han existido desde varios años atrás, una serie de ilícitos cometidos a través de las tarjetas de crédito/débito, concretamente el llamado "Skimming" o conocido como fraude con tarjetas de crédito y débito, su función radica cuando la persona víctima realiza un pago en un local comercial cualquiera con una tarjeta, la misma que al entregarla, la pierde de vista, en ese momento el delincuente informático que podría ser el propio mesero de un restaurante, pasa tal instrumento privado por un dispositivo conocido como skimmer, el cual almacena los códigos consignados en la tarjeta, para luego ser entregada esta información a un segundo sujeto activo, quien descarga la misma en un computador, finalmente los datos obtenidos se los graba en otro plástico o tarjeta en blanco, es así de esta manera en que el delincuente queda listo para realizar compras o transacciones a nombre del titular, configurándose así el delito de falsificación informática de instrumento privado, tarjeta de crédito.

4.3.4. FRAUDE, ESTAFA INFORMÁTICOS

Fraude informático, es: "el conjunto de conductas maliciosas, que valiéndose de cualquier manipulación fraudulenta, modifiquen o interfieran el funcionamiento de un programa informático, sistema

informático, sistema telemático o alguna de sus componentes, para producir un perjuicio económico de cualquier índole"45.

El fraude informático, "puede consistir en la adulteración del saldo de una cuenta, en una transferencia apócrifa, en la concesión de crédito a entidades inexistentes o insolventes o en otros manejos de naturaleza semejante"46.

Las Naciones Unidas, señalan tres tipos de fraudes informáticos, que "se puede dar en los datos de entrada –input- que constituyen la fase de suministro o alimentación de datos, en los datos de salida –output-, en el procesamiento de datos –programas-…"47, así:

- Manipulación de datos de entrada.

También se la conoce como "sustracción de datos". Este tipo de delito lo puede cometer cualquier sujeto, únicamente al saber los comandos requeridos para intervenir en el sistema informático o telemático y trasladar los fondos de una cuenta de otro sujeto.

45 ACURIO, Santiago. Ruptura por la legalidad. F&R Gráficas. Quito Ecuador. 2001. Pág.318
46 GUIBOURG, Ricard;Alende, Jorge;Campanella, Elena. Manual de Informática Jurídica. Astrea. Buenos Aires, Argentina.1996. Pág.275
47 MÁRQUEZ, Carlos. El Delito Informático. La Información y la Comunicación en la Esfera Penal. Editorial Leyer. Bogotá Colombia. 2002. Pág.273

- Manipulación de datos de salida.

Se efectúa con la tarea de fijar el funcionamiento del sistema, introduciendo instrucciones u órdenes falsas, las cuales el computador las recibe como ciertas, ejecutando una acción normalmente.

La comisión de esta acción, se da a través de los cajeros automáticos, tarjetas de crédito y débito.

- Manipulación de programas.

Esta conducta consiste en "modificar programas existentes en el sistema de la computadora o en insertar nuevos programas o nuevas rutinas, al programa computacional. Con esto, se busca desorientar las funciones del programa para buscar beneficio o aprovechamiento propio".

Para esta manipulación es necesario que el sujeto activo de la infracción posea altos conocimientos técnicos en informática, en especial programación.

Los fraudes informáticos, pueden surtir efecto mediante el manejo y uso de un sistema de interconexión de redes, llamado internet, el cual, gran parte de la población lo utiliza para un sinnúmero de actividades. Precisamente a través del correo electrónico, se genera una de las mayores estafas informáticas, esta consiste en enganchar a incautos

lectores del correo, pidiendo su ayuda para realizar una transacción, donde supuestamente obtendría un beneficio suculento. Pero la realidad es, que aparentemente para recibir el premio o ganancia, le solicitan el envío de los datos de una tarjeta de crédito, y el sujeto al enviarlos, más bien consigue ser estafado, porque el beneficio nunca llega, y los datos van a ser de objetivos maliciosos.

Otra modalidad de fraude informático actual, resulta de la creación de programas o páginas web de entidades bancarias, que al ojo humano pasan imperceptibles, sin que el usuario o cliente de esta institución, esté al corriente siquiera que no se trata de una página verídica. Es por esto que al solicitarles números de cuentas, números de las tarjetas de débito o crédito, y más aún al ingresar las claves o contraseñas, el delincuente informático se aprovecha de los datos ingresados, incorporándolos en la página real del banco, haciendo transacciones de dinero sin ningún control, perjudicando al ingenuo usuario, que no tiene conocimiento del ilícito que es víctima y peor de la identidad del victimario.

4.3.5. VIOLACIÓN A LA PRIVACIDAD PERSONAL

González Guitián, sostiene que la intimidad "debe ser un bien jurídico protegido, sencillamente porque la total falta de ella supone el absoluto e inmediato acceso, el conocimiento y la constante observación de un

individuo…, privándosele en consecuencia de su individualidad y, en definitiva, de su dignidad humana"48.

Todos tenemos derecho de mantener un espacio de privacidad sobre nuestras informaciones, las cuales no pueden estar en evidencia o al ojo de otros sujetos. Es la privacidad personal un derecho que se alza sobre otros, el de mantener bajo reserva datos privados, y si terceras personas los hicieren conocer, deben contar con la respectiva autorización o voluntad de su titular.

Eduardo Novoa Monreal, sustenta que la intimidad "es el espacio de la personalidad de los sujetos que no pueden ser por ningún motivo, salvo la propia elección, de dominio público. "…considera que la intimidad busca proteger el espacio privado, y se estructura como un derecho protector frente a las injerencias del Estado y de los particulares en la esfera privada"49.

El derecho a la privacidad equivale o lo podemos tomar como sinónimo del término "intimidad", que en sentido estricto se refiere a la información íntima y reservada de una persona.

48 JIJENA, Renato. Chile, la Protección Penal de la Intimidas y el Delito Informático. Editorial Jurídica de Chile. Santiago de Chile.1992.Pág.19,20
49 MÁRQUEZ, Carlos. El Delito Informático. La Información y la Comunicación en la Esfera Penal. Editorial Leyer. Bogotá Colombia. 2002. Pág.48

Vittorio Frosini, dice "que la intimidad reviste verdaderamente un valor positivo, en cuanto su contenido está integrado por facultades de control de las informaciones personales que circulan en la sociedad, sobre todo de los daros personales automatizados. Estas facultades, por ejemplo, serían los derechos de acceso, anulación, corrección y actualización ejercidos sobre la circulación de datos"50

La privacidad personal o la intimidad en consecuencia equivale al fuero interno de la persona y a su accionar, comprendiendo la esfera de su conducta, dejando bajo su reserva el conocimiento sobre sí mismo, o que determinadas personas tengan acceso.

La doctrina jurídica y el derecho han delineado ciertos principios básicos del derecho a la privacidad que los señalo a continuación:

a) Derecho al Conocimiento, el ciudadano, tiene derecho de conocer en dónde constan sus datos personales.

b) Derecho de Corrección, la persona tiene la posibilidad de pedir la rectificación de información errada.

50 JIJENA, Renato. Chile, la Protección Penal de la Intimidas y el Delito Informático. Editorial Jurídica de Chile. Santiago de Chile.1992. Pág.19,20

c) Derecho de Actualización, el ciudadano requieran que sus datos personales sean actualizados

d) Finalidad para la recolección, los sujetos interesados deben ser informados sobre los datos que se recolectan y por lo tanto, no pueden ser objetos de exposición o de una finalidad diferente a la que en un principio se estableció.

e) Calificación y no divulgación, hay que aclarar que no todos los datos son privados; siendo preciso manifestar que no se los debe divulgar y si se los hace, se estaría violando la privacidad personal.

f) “Seguridad de los Datos. La información tiene que encontrarse adecuadamente protegida en los registros en los que se la almacene.

“El derecho a la intimidad fue un enunciado que surgió en el año 1891 con motivo de un procedimiento penal instaurado por Samuel D. Warren y Louis D. Brandes, luego de que el primero de los nombrados fuera objeto en diversos diarios de notas sensacionalistas relacionadas con su vida privada. Con motivo de tal procedimiento, Warren y Brandes escribieron un opúsculo que titularon "The Right to Privacy", en donde decían que "el

individuo debía tener una completa protección de su persona y propiedades es un principio tan viejo como el 'common law'; pero se ha visto necesario de tiempo en tiempo, definir la exacta naturaleza y alcance de tal protección, Cambios políticos, sociales y económicos conllevan al reconocimiento de nuevos derechos, y el 'common law', en su eterna juventud, crece para satisfacer las demandas de la sociedad... Gradualmente se ha ido ensanchando el alcance de estos derechos, y ahora el derecho a la vida ha llegado a significar el derecho a disfrutar la vida –el derecho a ser dejado en paz–, el derecho a la libertad asegura el ejercicio de amplios privilegios civiles; y el término 'propiedad' ha llegado a comprender toda forma de posesión, tanto tangible, como intangible"51.

"No se puede dejar de reconocer que el Estado tiene derecho a conocer los datos relacionados con sus habitantes en tanto en cuanto los mismos sirvan rara fines sociales, pues estos datos pertenecen a la sociedad, en tanto el individuo vive en ella y se vale de ella para desarrollar su vida y para tener la máxima protección. Pero los datos personales deben ser diferenciados tomando en consideración los aspectos antes mencionados; y de ello surge la diferencia entre datos "públicos", que pertenecen a la

51 CRIMINOLOGIA E INFORMATICA.- La informática y el derecho a la intimidad.- Jorge Zavala Baquerizo.- Pág. 5

sociedad y de los cuales se puede servir el Estado; y datos privados, esto es, aquellos a los que el pensamiento suizo que elaboró el proyecto destinado a la protección de los bancos de datos, denominó "datos sensibles". Entre los públicos se encuentran los datos referidos al nombre, residencia, número de identidad personal, profesión, estado civil, lugar de trabajo, etc. Entre los segundos, o privados, tenemos la religión, la opinión política, el estado de salud, su posición económica, etc.

De lo dicho se llega, pues, a la conclusión de que las personas, cuyos datos individuales, sin discriminación entre públicos y privados, están dentro de un banco de datos, se encuentran indefensas en cuanto al resguardo de su intimidad y la de su familia, pues el manipuleo de la información puede provocar graves lesiones a los intereses, no sólo del individuo, sino también de toda su familia. Los autores argentinos Carlos Correa, Hilda N. Batto, Susana Czar de Zalduendo y Félix A. Nazar, en su obra conjunta "Derecho Informático", nos recuerdan lo sucedido en su país durante la trágica dictadura militar última que sufrió dicha Nación. Ellos nos dicen: "En épocas recientes de nuestro país, la acumulación de datos personales en un Estado autocrático, privó a los individuos de toda posibilidad de verificar los datos que sobre ellos se poseían. La manipulación de datos sobre convicciones políticas y religiosas, el recurso a informaciones obsoletas (pertenencia en épocas pretéritas a un centro estudiantil o partido político, etc.), fueron con

frecuencia la base de acciones represivas y aberrantes violaciones de los derechos humanos". De lo dicho surge la necesidad que tiene el ciudadano de hoy de controlar la información que, sobre su persona, contienen los diversos bancos de datos, a fin de proteger su intimidad y la de su familia. Y de esta conclusión se hace presente la necesidad de que existan la suficiente legislación que permita el control de los bancos de datos y el derecho a que se supriman los considerados privados, y se rectifiquen los públicos que se consideren obsoletos o equivocados"52.

4.4. CAPITULO IV.- LEGISLACIÓN COMPARADA

4.4.1 EL DELITO INFORMÁTICO EN EL CÓDIGO PENAL ECUATORIANO.

Nuestro Código Penal contiene los siguientes delitos informáticos: Delitos contra la Información Protegida: Violación de claves o sistemas de seguridad; Delitos contra la Información Protegida: Destrucción o supresión de documentos, programas; Falsificación Electrónica; Daños Informáticos; Fraude Informático; Violaciones al Derecho a la Intimidad y Pornografía Infantil, a continuación su detalle:

1.- Delitos contra la Información Protegida: Violación de claves o sistemas de seguridad

52 CRIMINOLOGIA E INFORMATICA.- La informática y el derecho a la intimidad.- Jorge Zavala Baquerizo.- Pág. 8 - 9

Título II: DE LOS DELITOS CONTRA LAS GARANTIAS CONSTITUCIONALES Y LA IGUALDAD RACIAL.

Cap. V. De los Delitos Contra la inviolabilidad del secreto.

Art. 202.- inclúyanse los siguientes artículos innumerados:

Artículo... (202.1).- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

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

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

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

Artículo... (202.2).- Obtención y utilización no autorizada de Información.- La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.

Estas disposiciones conllevan una serie de elementos claves en la configuración del delito informático, la presencia de un sujeto activo quien es el que atenta contra el sistema de información, vulnerando las seguridades de este, el sujeto pasivo quien es el titular de la información protegida y el bien jurídico que representa la confidencialidad, reserva de la información. Así también como la presencia del instrumento a través del cual se perpetúa el delito informático, un medio informático o electrónico. Todo esto representa el tipo penal, y la respectiva sanción que se establece contra quienes realizan esta clase de ilícitos. Pero se

observa claramente, que al respecto del delito de la utilización no autorizada de información, en donde el titular autoriza o no el uso de su información, si bien se castiga a quienes son los autores de este ilícito, más no se hace referencia, a que en el cometimiento de este delito, muchas veces cuenta con la autorización de su titular, claro es el ejemplo de la suplantación de identidad, falsificando un instrumento público, convirtiéndose así esta persona en autor y cómplice de un delito contra sí mismo.

2.- Delitos contra la Información Protegida: Destrucción o supresión de documentos, programas.

TITULO III. DE LOS DELITOS CONTRA LA ADMINISTRACION PÚBLICA. Cap. V. De la Violación de los deberes de Funcionarios Públicos, de la Usurpación de Atribuciones y de los Abusos de Autoridad. Artículo 262.- Serán reprimidos con 3 a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados en razón de su cargo.

En este articulado, se señala al funcionario público y por lo tanto su posible participación en una infracción de este tipo, así mismo la sanción que se apega a la realidad legal, este empleado al ocupar un cargo y manejar información privada en ciertos casos, el legislador lo ha visto dentro del campo de posibles acciones maliciosas.

3.- Falsificación Electrónica

Título IV. DE LOS DELITOS CONTRA LA FE PUBLICA.- Cap. III. De las Falsificaciones de Documentos en General.

Art. 353.- Agréguese el siguiente artículo innumerado:

Artículo… (353.1).- 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:

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

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

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

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

Esta normativa abarca especial significación en mi estudio de este capítulo; la doctrina, jurisprudencia penal enseña que una norma penal consta del tipo penal y la respectiva sanción, respecto al primer componente está claro o al menos el legislador en base a otras legislaciones ha transcrito lo sustancial al tema de la falsificación informática, pero como siempre no es suficiente; en cuanto al segundo componente, se advierte la no existencia de una sanción contra quienes cometen este delito, sólo se direcciona a decir que las sanciones estarán de acuerdo a lo que dispone ese capítulo. Esa poca o nula normativa penal no puede caber o registrar nuestra legislación, cada norma debe tener sus preceptos y conceptos bien establecidos y regulados, destinando a cada ilícito una respectiva sanción.

4.- Daños Informáticos

Titulo V. DE LOS DELITOS CONTRA LA SEGURIDAD PÚBLICA. Cap. VII:- Del incendio y otras Destrucciones, de los deterioros y Daños

Art. 415.- Inclúyanse los siguientes artículos innumerados:

Artículo… (415.1).- Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

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

Artículo... (415.2).- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seis cientos dólares de los Estados Unidos de Norteamérica.

Estos artículos puestos en consideración en el campo de los delitos informáticos, revisten de cierta realidad, no muy apegada a una verdad, en el sentido que los delincuentes informáticos, al menos en nuestro país, no han ingresado en programas, informaciones o bases de datos con la intención de destruirlos, no es muy conocida o difundida esta situación, lo que busca en realidad este sujeto activo es la obtención de réditos económicos a través de su ilícito. De todas formas, es necesaria su configuración dentro del campo penal por posibles atentados en las bases de datos e informaciones públicas y privadas.

5.- Fraude Informático

Titulo X. De los Delitos contra la Propiedad.

Cap. V De las Estafas y otras defraudaciones.

Art. 553.- Añádanse los siguientes artículos innumerados:

Artículo… (553.1).- Apropiación Ilícita.- Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o

modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

Artículo… (553.2).- La pena será de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

1.- Inutilización de sistemas de alarma o guarda;

2.- Descubrimiento o descifrado de claves secretas o encriptadas;

3.- Utilización de tarjetas magnéticas o perforadas;

4.- Utilización de controles o instrumentos de apertura a distancia;

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

Artículo 563.- inciso segundo:

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

6.- Violaciones al Derecho a la Intimidad (Contravención)

LIBRO III. TITULO I. CAP. III. DE LAS CONTRAVENCIONES DE TERCERA CLASE.

Artículo 606.- numeral 19

Serán reprimidos con multa de siete a catorce dólares de los Estados Unidos de Norteamérica y con prisión de dos a cuatro días, o con una de estas penas solamente: 19.Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

7.- Pornografía Infantil

Título VIII, Capítulo III.1, De los Delitos de Explotación Sexual.

Artículo… (528.7).- Quien produjere, publicare o comercializare imágenes pornográficas, materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato u organizare espectáculos en vivo, con escenas pornográficas en que participen los mayores de catorce y menores de dieciocho años será reprimido con la pena de seis a nueve años de reclusión menor ordinaria, el comiso de los objetos y de los bienes productos del delito, la inhabilidad para el empleo profesión u oficio.

Con la misma pena incurrirá quien distribuyere imágenes pornográficas cuyas características externas hiciere manifiesto que en ellas se ha grabado o fotografiado la exhibición de mayores de doce y menores de dieciocho años al momento de la creación de la imagen.

Con la misma pena será reprimido quien facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico en cuyas imágenes participen menores de edad.

Cuando en estas infracciones, la víctima sea un menor de doce años o discapacitado, o persona que adolece enfermedad grave incurable, la pena será de reclusión mayor extraordinaria de doce a dieciséis años, al pago de la indemnización, el comiso de los objetos y de los bienes producto del delito, a la inhabilidad del empleo, profesión u oficio; y, en caso de reincidencia, la pena será de veinticinco años de reclusión mayor especial.

Cuando el infractor de estos delitos sea el padre, la madre, los parientes hasta el cuarto grado de consanguinidad y segundo de afinidad, los tutores, los representantes legales, curadores o cualquier persona del contorno intimo de la familia, los ministro de culto, los maestros y profesores y, cualquier otra persona por su profesión u oficio hayan abusado de la víctima, serán sancionados con la pena de dieciséis o veinticinco años de reclusión mayor extraordinaria, al pago de la indemnización, el comiso de los objetos y de los bienes producto del delito de inhabilidad del empleo u oficio. Si la víctima fuere menor de doce años se aplicará el máximo de la pena.

4.4.2 DELITO INFORMÁTICO EN LA LEY DE COMERCIO ELECTRÓNICO.

La ley de Comercio Electrónico, Firmas y Mensajes de Datos creada por el Congreso Nacional y que rige en nuestro país desde el 27 de febrero de 2002, Registro Oficial 557, se implanta por la necesidad de contar con una herramienta o normativa jurídica especializada en la materia de informática reguladora de una serie de hechos suscitados en la actualidad, refiriéndome a las tendencias de comunicación e intercambio comercial a través de la red, mismas que se han desarrollado de manera vertiginosa, donde es posible concebir una sociedad en donde la estructura de una relación comercial, se lleve a cabo con el uso de un sistema telemático o informático. En síntesis, esta ley, se encamina a regular y controlar el uso de los servicios de redes electrónicas, el internet y las relaciones de comercio a través de actos y contratos informáticos.

Ahora resulta, que si bien esta ley en su articulado establece como objeto, regular:

- mensajes de datos, entendidos como la elaboración, transferencia, utilización de datos y la correspondiente voluntad y consentimiento expreso de su titular para el uso de terceros;
- documentos electrónicos, validez legal al igual que otros documentos públicos o privados, facilitando el intercambio de información y a la vez permitirnos efectuar transacciones electrónicas, facturar por medio electrónicos, etc;
- la firma electrónica, su carácter y requisitos de validez, existencia y utilidad en un contrato informático, al igual que la firma manuscrita; y,
- el comercio electrónico, con sus características de fondo, forma y la manera de proceder para conseguir un resultado satisfactorio en esta relación contractual, intercambiando los mensajes de datos o que la compra en sitios web en Internet sean válidos, con efectos comerciales y jurídicos, iguales a los contratos por escrito.

Mas en su normativa final, a partir del artículo 57 hasta el 67, final, se ha hecho hincapié en crear disposiciones que normen de alguna forma las infracciones informáticas, las cuales se suscitan cuando el objeto jurídico que esta ley consagra es atentado o alterado y su sujeto pasivo se convierte en víctima de violaciones y lesiones a sus derechos. Esta

normativa final de la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, se creó para modificar la normativa del Código Penal y en especial, sancionar los delitos detallados a continuación:

1.- divulgación y violación del derecho a la intimidad en documentos o información electrónica protegida (Art. 58 y 64);

2.- obtención y utilización no autorizada de información (Art. 58);

3.- destrucción o supresión de documentos o información electrónica, por parte de personas que los tuvieren su cargo (Art. 59);

4.- falsificación electrónica (Art. 60);

5.- daños informáticos (Art. 61);

6.- apropiación ilícita (Art. 62);

7.- estafa, a través de medios electrónicos o telemáticos (Art. 63);

4.4.3.- COMPARACIÓN CON LA LEGISLACIÓN DE ARGENTINA

En la legislación penal argentina, específicamente en el Código Penal, se ha puesto énfasis por parte de los legisladores argentinos en crear una normativa clara, ante el problema social alarmante de los delitos informáticos, y dentro de estos la falsificación informática, con las ya conocidas consecuencias destructivas en el ámbito económico y de la privacidad personal. En este sentido, se han hecho reformas al Código, que permiten contar con un cuerpo legal que abarque los campos del

posible delito informático. No obstante requiere que los legisladores creen una legislación con mayor profundidad y análisis, para no dejar cabos sueltos en este tema. A continuación realizo un enfoque de las normas contenidas y que representan o se relacionan con el delito informático.

Dentro de este Código Penal, se puede apreciar el delito de violación de secretos y de la privacidad, tipificando en su artículo 153, que "será reprimido con prisión de 15 días a seis meses el que abriere o accediere indebidamente a una comunicación electrónica,… …que no le esté dirigido; o se apoderare indebidamente de una comunicación electrónica; o indebidamente suprimiere o desviare de su destino… …una comunicación electrónica que no le esté dirigida. En la misma pena incurrirá el que indebidamente interceptare o captare comunicaciones electrónicas o telecomunicaciones proveniente de cualquier sistema de carácter privado o de acceso restringido. La pena será de prisión de un mes a un año, si el autor además comunicare a otro o publicare el contenido de la… …comunicación electrónica. Si el hecho lo cometiere un funcionario público… …sufrirá además, inhabilitación especial por el doble del tiempo de la condena". Con esta norma jurídica, observamos que este delito encaja perfectamente dentro del delito informático en general. El término comunicación electrónica, lo asociamos o relacionamos con los mensajes de datos, mails o correos electrónicos, que se envían o receptan por medio de un computador o en base a un sistema informático. Sin la autorización del titular, ninguna persona puede

acceder o desviarles de su destino a tales comunicaciones. A la hora de establecer una sanción el legislador ha puesto de manifiesto las sanciones respectivas a los autores de este delito, dentro de los cuales se destacan cualquier persona en ejercicio de sus funciones privadas, y también se sanciona a los funcionarios públicos como entes de posibles delincuentes informáticos, quienes podrían atentar contra los datos que tienen bajo su custodia o la información privada su cargo. Con el artículo 153 bis, concretamente se amplía lo manifestado anteriormente al tipificar el tipo penal y la sanción al "…que a sabiendas accediere por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema o dato informático de acceso restringido". En la esfera estatal, dicho Código Penal, en un inciso del mismo artículo 153, hace referencia a la pena de "…un mes a un año de prisión cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros. Toda esta normativa abarca los posibles campos de acción y consumación de este delito, evitando caer en ello, o advirtiendo que existe una legislación que norma y castiga a los delincuentes, cómplices y encubridores de esta clase de infracción.

En el Código Penal ecuatoriano, en su artículo 220 si bien se advierte sobre las sanciones a la persona que acceden a una base de datos restringida sin la voluntad de su titular, mas no determina en cuanto al funcionario público, como posible sujeto activo de este delito.

En el artículo 155 del código penal argentino, asimismo castiga a los sujetos activos del delito de indebida publicación de información, reprimiendo "con multa de un mil quinientos pesos a cien mil, el que hallándose en posesión de una correspondencia, una comunicación electrónica, …, no destinados a la publicidad, los hiciere publicar indebidamente, si el hecho causare o pudiere causar perjuicios a terceros". De igual forma, podemos apreciar que para la existencia del delito informático, debe haber una acción ilícita sobre un sistema de información, en este caso sobre una comunicación electrónica, y el mal uso que se le da, al publicar una información no autorizada publicación, sin saber las consecuencias que podría traer consigo, y mucho más a sabiendas del mal que causa, es justo el castigo se impone.

El artículo 157, sanciona a los funcionarios públicos con prisión de un mes a dos años e inhabilitación especial de uno a cuatro años, por sus actuaciones indebidas, revelando secretos de hechos, datos protegidos por la ley, secretos que pudieren causar alarma social o perjudicar a personas inocentes. En este sentido, existen violaciones a la privacidad personal, específicamente dirigidas contra los datos personales de los sujetos pasivos del delito de acceso indebido a la información, estudio y análisis este artículo contiene una norma ampliatoria, la cual indica en el "Art. 157 bis. Será reprimido con la pena de prisión de un mes a dos años el que: 1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de

datos, accediere, de cualquier forma, a un banco de datos personales; 2. Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley. 3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años". Esta normativa está encaminada a poner fin a las actuaciones de las instituciones públicas, el Registro Civil por ejemplo, una entidad encargada del manejo y procesamiento de datos personales, y cuyas funciones realizadas por sus respectivos empleados, se encaminan a la correcta aplicación de sus actividades, sin embargo la codicia, el interés de ganar réditos económicos, les lleva a cometer actos delictivos, a sabiendas del daño, de lo incorrecto que es eso. Pero la legislación penal, no deja en una simple descripción de este hecho, por el contrario busca dar un término a lo ilícito, al castigar a sus infractores, tanto quienes están dentro de la función pública, como aquellos que están desde fuera favoreciendo este cometimiento.

Ahora hacemos referencia a la falsificación informática, parte del título del tema de mi tesis, con la cual se deja de manifiesto, que la legislación argentina establece los parámetros claros sobre este delito. En primer lugar señalo lo que el capítulo uno del Código Penal argentino establece: "Falsificación de moneda, billetes de banco, títulos al portador y documentos de crédito.

Dentro de este capítulo se estipula lo concerniente a la falsificación de la moneda de la República, con sus respectivas sanciones, por ejemplo el artículo 282, indica que "Será reprimido con reclusión o prisión de tres a quince años, el que falsificare moneda que tenga curso legal en la República y el que la introdujere, expendiere o pusiere en circulación", asimismo en el artículo 283 castiga "con reclusión o prisión de uno a cinco años, el que cercenare o alterare moneda de curso legal y el que introdujere, expendiere o pusiere en circulación moneda cercenada o alterada. En fin estos artículos conllevan lo referente a la moneda, pero ahora es preciso señalar lo que el artículo 285 pone de manifiesto al dejar "…equiparados a la moneda nacional, la moneda extranjera, los títulos de la deuda nacional, provincial o municipal y sus cupones, los bonos o libranzas de los tesoros nacional, provinciales y municipales, los billetes de banco, títulos, cédulas, acciones, valores negociables y tarjetas de compra, crédito o débito, legalmente emitidos por entidades nacionales o extranjeras autorizadas para ello,…". Ahora pues, queda claro que esta normativa, sí hace referencia a la falsificación informática, porque un instrumento privado como las tarjetas de crédito, al ser objeto de falsedad, constituyen una acción ilícita, en el sentido que su origen se basa en un conjunto de actividades encaminadas a generar un perjuicio. Es entonces fácil cambiar el sentido e intercambiar la frase moneda nacional por instrumento privado o público, y bien sabemos que la falsificación de estos documentos, se los hace a través de un ordenador o sistema informático.

En segundo lugar señala sobre la falsificación de documentos en general en el Capítulo 3, artículo 292, haciendo hincapié en reprimir al delincuente falsificador con "reclusión o prisión de uno a seis años, si se tratare de un instrumento público y con prisión de seis meses a dos años, si se tratare de un instrumento privado", el documento verdadero que es objeto de adulteración o, el documento que se lo falsifica en todo o en parte, y que obviamente vaya generar un perjuicio; para hablar de perjuicio, podemos catalogarlo como el daño económico o moral contra un sujeto. En cuanto a las sanciones establecidas, debería establecerse a más de las medidas personales, las medidas reales en esta disposición, puesto que el instrumento privado cuenta con un tiempo de castigo menor para quienes atentan contra este documento, y donde la pérdida económica podría ser significativa, como en el caso de la falsificación de tarjetas de crédito; a diferencia del documento público, donde la sanción está dentro de los estamentos de la gravedad que representa esta infracción, equiparando la lesión con el castigo, concretando la falsedad o ejercida por ejemplo en una libreta militar, pasaporte, partida de nacimiento o cédula de ciudadanía; este último, instrumento representante de la identidad y existencia de un sujeto, y también posible objeto de alteraciones o modificaciones atentatorias contra la víctima de tal ejecución. El artículo 293, sanciona con penas de tres a ocho años si en estos instrumentos, se introdujeren declaraciones falsas de la identidad personal o se crearen

documentos privados con información falsa, para efectuar un perjuicio, como el delito de robo de identidad o robo de dinero.

En segundo lugar, en este capítulo interviene la inserción de declaraciones falsas dentro de un instrumento público en el artículo 293, esta situación refiere a las declaraciones malintencionadas o falsas constantes en una escritura pública, instrumento legal otorgado ante la autoridad respectiva, y cuya edificación conlleva una sanción, que consiste en la reclusión o prisión de uno a seis años. Dentro de la sociedad argentina, existen certificados de adquisición de ganado u otros documentos que representan la propiedad sobre estos semovientes, los cuales son emitidos por una autoridad pública, quien debe tomar las medidas necesarias para cerciorarse de la procedencia de estos bienes, pero si no observa esta disposición, se le impondrá la prisión de uno a tres años.

En este cuerpo legal del artículo 295 al 296, se expone el delito de otorgamiento de documentos falsos por parte de un profesional, un médico, pronunciando una sanción para este, así como para quien hace uso de tal instrumento, es una norma que por fin abarca tanto al autor como al ejecutor de esa infracción, con la cual quedamos de acuerdo en su totalidad.

El artículo 299, penaliza con "…prisión de un mes a un año, el que fabricare, introdujere en el país o conservare en su poder, materias o instrumentos conocidamente destinados a cometer alguna de las falsificaciones legisladas…", esto significa que existen materiales u objetos electrónicos, útiles en la perpetración de la falsificación informática; aunque específicamente así no lo menciona, pero sí lo podemos deducir de lo tipificado, con este análisis podemos apreciar que esta legislación extranjera sí advierte o contiene lo relativo a la falsificación informática, mientras que nuestro código penal es nulo en normar lo relacionado con en este párrafo.

4.4.4 COMPARACIÓN CON LA LEGISLACIÓN DE ESPAÑA.

Para una mejor comprensión de este capítulo, es necesario primero advertir que en cuanto a las penas aplicadas por delitos cometidos, el legislador español, las ha determinado según el artículo 50 del Código Penal español, como el sistema de días-multa, lo que representa una extensión mínima de 10 días y máxima de 2 años para las personas naturales, en tanto que a las personas jurídicas la extensión será de 5 años. Asimismo la pena pecuniaria para las personas naturales tendrá un mínimo de 2 y máximo de 400 euros, mientras que para las jurídicas la cuota diaria será mínimo de 30 y máximo de 5.000 euros. Esta

explicación, a la hora de encontrar en las normas siguientes, penas y multas contadas en días, meses y años.

El código penal español, establece una normativa referida a la violación al derecho a la intimidad, imagen y domicilio de una persona. Esto constante dentro del:

LIBRO II. DELITOS Y SUS PENAS

TÍTULO X. DELITOS CONTRA LA INTIMIDAD, EL DERECHO A LA PROPIA IMAGEN Y LA INVIOLABILIDAD DEL DOMICILIO

CAPÍTULO PRIMERO. DEL DESCUBRIMIENTO Y REVELACIÓN DE SECRETOS

Artículo 197

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

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

3. El que por cualquier medio o procedimiento y vulnerando las medidas de seguridad establecidas para impedirlo, acceda sin autorización a datos o programas informáticos contenidos en un sistema informático o en parte del mismo o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

4. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.

5. Si los hechos descritos en los apartados 1 y 2 de este artículo se realizan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros, se impondrá la pena de prisión de tres a cinco años, y si se difunden, ceden o revelan los datos reservados, se impondrá la pena en su mitad superior.

6. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o un incapaz, se impondrán las penas previstas en su mitad superior.

Artículo 198.- La autoridad o funcionario público que, fuera de los casos permitidos por la ley sin mediar causa legal por delito, y prevaliéndose de su cargo, realizare cualquiera de las conductas descritas en el artículo anterior, será castigado con las penas respectivamente previstas en el mismo, en su mitad superior y, además, con la de inhabilitación absoluta por tiempo de seis a doce años.

A diferencia del Código Penal ecuatoriano, el presente cuerpo legal español, establece un andamiaje jurídico completo en cuanto a la violación en definitiva al derecho a la privacidad personal, mientras el primero lo cataloga como una mera contravención en el derecho penal ecuatoriano, el segundo lo catapulta como un delito que afecta y produce graves consecuencias en la intimidad de un sujeto español. Haciendo un análisis de cada uno de los puntos que constituyen este ilícito, puesto que no se queda sólo en el delito de acceso a tales informaciones contenidas en un soporte informático, sino que además plasma lo concerniente a la divulgación y revelación de tales datos, sancionando con penas específicas a cada uno de ellos. Las sanciones en sí, van encaminadas a penar, tanto a las personas ajenas o familiares que acceden a los documentos informáticos de su víctima, como a las personas que tienen a su cargo dichos instrumentos y los utilizan para perjudicar a terceros. Es también claro que el campo de acción y sus enfoques se los señala en los ámbitos de ideología, religión, creencias, salud, origen racial o vida sexual de un sujeto, cubriendo así los ámbitos que constituyen un ente humano, permitiendo al juzgador actuar de una manera proclive y justa; en definitiva el legislador español ha contribuido con una cuerpo penal suficiente a la hora de buscar el tipo de delito cometido y al momento de sancionar al o a los culpables, que van a ser una persona cualquiera o los

mismos funcionarios públicos, encargados de la administración de una base de datos o de informaciones personales reservadas.

SECCIÓN PRIMERA. De las estafas

Artículo 248

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

2. También se consideran reos de estafa:

a) Los que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consigan una transferencia no consentida de cualquier activo patrimonial en perjuicio de otro.

b) Los que fabricaren, introdujeren, poseyeren o facilitaren programas informáticos específicamente destinados a la comisión de las estafas previstas en este artículo.

c) Los que utilizando tarjetas de crédito o débito, o cheques de viaje, o los datos obrantes en cualquiera de ellos, realicen operaciones de cualquier clase en perjuicio de su titular o de un tercero.

Artículo 249.- Los reos de estafa serán castigados con la pena de prisión de seis meses a tres años, si la cuantía de lo defraudado excediere de 400 euros. Para la fijación de la pena se tendrá en cuenta el importe de lo defraudado, el quebranto económico causado al perjudicado, las relaciones entre éste y el defraudador, los medios empleados por éste y cuantas otras circunstancias sirvan para valorar la gravedad de la infracción.

Esta sección establece lo tipificado a las estafas, a pesar de que no esté titulada como informática, es claro su compendio y su esencia, al señalar la existencia de la manipulación informática, la cual produce un delito

informático que como ya lo hemos estudiado constituye la estafa informática, esta es la denominada técnica de salami, que el literal "a" la imprime. Igualmente el literal "b", se lo relaciona con el delito informático conocido como técnica de salami, que son la introducción de programas informáticos con el fin mismo de estafar a los sujetos pasivos. Y el último literal, es el uso de un instrumento privado para hacerle un daño a su titular, el denominado skimming. Aquí, a la hora de sancionar a los culpables se implantan parámetros punibles, consistentes en fijar la respectiva pena de acuerdo al daño ocasionado, es decir al perjuicio económico, a las circunstancias y a los medios utilizados en la perpetración del delito. Esta normativa nos enseña que las estafas informáticas, se generan mediante un proceso lógico, sistematizado y consciente de la generación de grandes daños en la economía y patrimonio de las posibles víctimas.

SECCIÓN TERCERA. De los delitos relativos al mercado y a los consumidores

Artículo 278

1. El que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del art. 197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

2. Se impondrá la pena de prisión de tres a cinco años y multa de doce a veinticuatro meses si se difundieren, revelaren o cedieren a terceros los secretos descubiertos.
3. Lo dispuesto en el presente artículo se entenderá sin perjuicio de las penas que pudieran corresponder por el apoderamiento o destrucción de los soportes informáticos.

Esta sección es simultánea con la divulgación de informaciones reservadas o secretos que el código penal ecuatoriano, sí lo traía a colación con la respectiva sanción; en el presente código en primer lugar, se ha puesto de manifiesto que este delito consiste en apoderarse de un documento informático y en segundo lugar, se impone una pena contra quienes difundan o revelen tales secretos. Muchas veces con la intención de apoderarse de un secreto de algún producto, se incurre en violentar las seguridades de un sistema para buscar y obtener esa reserva y así poder utilizarla a su beneficio o cederla a favor de terceros, produciendo un grave perjuicio en los autores del objeto, a este delito se lo conoce como acceso indebido a un sistema informático, y en el caso de que el autor no reciba retribución alguna por su autoría, se le conoce como piratería informática, y al difundirse tal producto en el mercado, el daño ocasionado es de mayor significancia aún para los consumidores, al no recibir un producto de calidad.

Artículo 286

1. Será castigado con las penas de prisión de seis meses a dos años y multa de seis a 24 meses el que, sin consentimiento del prestador de servicios y con fines comerciales, facilite el acceso inteligible a un servicio de radiodifusión sonora o televisiva, a servicios interactivos prestados a distancia por vía electrónica, o suministre el acceso condicional a los mismos, considerado como servicio independiente, mediante:

1º La fabricación, importación, distribución, puesta a disposición por vía electrónica, venta, alquiler, o posesión de cualquier equipo o programa informático, no autorizado en otro Estado miembro de la Unión Europea, diseñado o adaptado para hacer posible dicho acceso.

2º La instalación, mantenimiento o sustitución de los equipos o programas informáticos mencionados en el párrafo 1º.

2. Con idéntica pena será castigado quien, con ánimo de lucro, altere o duplique el número identificativo de equipos de telecomunicaciones, o comercialice equipos que hayan sufrido alteración fraudulenta.

3. A quien, sin ánimo de lucro, facilite a terceros el acceso descrito en el apartado 1, o por medio de una comunicación pública, comercial o no, suministre información a una pluralidad de personas sobre el modo de conseguir el acceso no autorizado a un servicio o el uso de un dispositivo o programa, de los expresados en ese mismo apartado 1, incitando a lograrlos, se le impondrá la pena de multa en él prevista.

4. A quien utilice los equipos o programas que permitan el acceso no autorizado a servicios de acceso condicional o equipos de telecomunicación, se le impondrá la pena prevista en el art. 255 de este Código con independencia de la cuantía de la defraudación.

Este articulado que nuestro código penal no lo tipifica, va a resguardar los servicios de radio y televisión prestados a través de vía electrónica o informática, es decir que la norma lo ampara para dar un servicio óptimo y castigar a quienes lo intervienen o acceden para provocar un daño. Pero esta situación no se la lleva a cabo con la simple presencia del sujeto activo de la infracción, es menester una herramienta, equipo o programa informático que faculte un delito completo. Es por esto que en esta norma jurídica, a más de sancionar a quienes acceden a violentar las telecomunicaciones, se castiga además a los sujetos que fabrican y ponen en comercialización estos aparatos. Este último punto es muy interesante e importante llevarlo a mención, ahí está presente el origen de la infracción y por consiguiente hay que castigar a los responsables de la producción de estos materiales que son usados ilegalmente.

TÍTULO XVIII. DE LAS FALSEDADES

CAPÍTULO II. DE LAS FALSEDADES DOCUMENTALES

SECCIÓN PRIMERA. De la falsificación de documentos públicos, oficiales y mercantiles y de los transmitidos por servicios de telecomunicación

En cuanto a las falsificaciones, debo dar una mención especial a nuestro Código Penal, que en contraposición del español, este último en ningún momento se refiere acerca de la falsificación electrónica ni informática.

Nuestros legisladores casi han copiado textualmente los numerales del artículo 390 del Código Penal espalo, pero lo encaminaron al ámbito informático, sin embargo esta normativa impresa a continuación, no se refiere a nuestro tema de estudio.

Artículo 390

1. Será castigado con las penas de prisión de tres a seis años, multa de seis a veinticuatro meses e inhabilitación especial por tiempo de dos a seis años, la autoridad o funcionario público que, en el ejercicio de sus funciones, cometa falsedad:

1º) Alterando un documento en alguno de sus elementos o requisitos de carácter esencial.

2º) Simulando un documento en todo o en parte, de manera que induzca a error sobre su autenticidad.

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

4º) Faltando a la verdad en la narración de los hechos.

Se puede catalogar como rescatable lo que los legisladores señalaron en esta norma, al tipificar en primer lugar la sanción a este delito. Lo malo es que nuestros legisladores, no copiaron y no hicieron énfasis en establecer la pena.

SECCIÓN CUARTA. De la falsificación de tarjetas de crédito y débito y cheques de viaje

Artículo 39.- 1. El que altere, copie, reproduzca o de cualquier otro modo falsifique tarjetas de crédito o débito o cheques de viaje, será castigado con la pena de prisión de cuatro a ocho años. Se impondrá la pena en su mitad superior cuando los efectos falsificados afecten a una generalidad de personas o cuando los hechos se cometan en el marco de una organización criminal dedicada a estas actividades.

Cuando de acuerdo con lo establecido en el art. 31 bis una persona jurídica sea responsable de los anteriores delitos, se le impondrá la pena de multa de dos a cinco años.

2. La tenencia de tarjetas de crédito o débito o cheques de viaje falsificados destinados a la distribución o tráfico será castigada con la pena señalada a la falsificación.

3. El que sin haber intervenido en la falsificación usare, en perjuicio de otro y a sabiendas de la falsedad, tarjetas de crédito o débito o cheques de viaje falsificados será castigado con la pena de prisión de dos a cinco años.

Esta sección tiene trascendencia en el ámbito de la falsificación informática, es cierto que la alteración, copia y reproducción de una tarjeta de crédito o débito, se la hace a través de un sistema informático o con el uso de aparatos idóneos y propicios creados para tal particular. Si bien es cierto que no se lo menciona como lo señalamos, pero es fácil deducir y concluir que a este delito se lo conoce a manera de falsificación informática de instrumento privado.

En nuestro ordenamiento penal, no existe normativa alguna acerca de este tema, mas es conocido por todas las personas, los ilícitos producidos durante los últimos años, y aquí encontramos que el código

penal español trae a bien tipificar este delito de producción masiva y muchas veces silenciosa. Las sanciones establecidas en el numeral uno, se enfocan a castigar individual y colectivamente, en general al grupo de individuos que forman una organización delictiva, siendo estos los sujetos que obtienen la tarjeta de crédito o débito de un titular y quienes con la ayuda de aparatos electrónicos configuran como tal la falsificación de ese instrumento. A más de las personas indicadas anteriormente, en el numeral tres se penaliza a los individuos que ya utilizan o ponen en funcionamiento tales documentos falsos, sin tener participación directa en el cometimiento de la falsificación.

En muchos casos, surgen delincuentes informáticos que sin tener la intención de provocar un daño financiero en la economía de una persona, tal vez ingenuamente ponen en manifiesto se deseo de utilizar un documento falso, sin tener en cuenta las repercusiones que mediata o inmediatamente acarrean. Es así que con el ánimo de sacar un provecho, utilizan estas tarjetas para una compra por ejemplo, y caen en delito flagrante. Esta situación tiene una diferente concepción, pero las legislaciones estudiadas y más la nuestra, hasta el momento no las ha catalogado ni señalado en sus normativas penales.

CAPÍTULO III. DISPOSICIONES GENERALES

Artículo 400.- La fabricación o tenencia de útiles, materiales, instrumentos, sustancias, máquinas, programas de ordenador o aparatos, específicamente destinados a la comisión de los delitos descritos en los Capítulos anteriores, se castigarán con la pena señalada en cada caso para los autores.

Artículo 536.- La autoridad, funcionario público o agente de éstos que, mediando causa por delito, interceptare las telecomunicaciones o utilizare artificios técnicos de escuchas, transmisión, grabación o reproducción del sonido, de la imagen o de cualquier otra señal de comunicación con violación de las garantías constitucionales o legales, incurrirá en la pena de inhabilitación especial para empleo o cargo público de dos a seis años.

Si divulgare o revelare la información obtenida, se impondrán las penas de inhabilitación especial, en su mitad superior y, además, la de multa de seis a dieciocho meses.

Dentro de las disposiciones generales, he tomado dos artículos se relacionan o refieren a los delitos informáticos, precisamente a los objetos o medios con los cuales se lleva a cabo un ilícito penal, el artículo 400, pone de manifiesto que la fabricación o tenencia de programas de ordenador para el cometimiento de cualquiera de los delitos señalados en el código penal español, es castigado con la respectiva pena a sus autores. En nuestro código penal, se debería advertir que todo ese proceso que abarca la fabricación y uso de esos aparatos, y en este caso de esos programas que cuando se los introduce en un sistema, dañan el normal funcionamiento o van dirigidos a sacar un provecho económico.

En el artículo 536, su conglomerado lo denominaremos Intervención o pinchado de las líneas de comunicación, delito informático que la doctrina lo menciona. Y que este cuerpo legal también lo ha hecho eco; se sanciona a la autoridad, funcionario público o agente de éstos, y a personas comunes y corrientes, anteriormente ya se los ha revestido de aplicación y ejecución en sus actos. Ahora se castiga a estos sujetos que dentro de sus actividades, llegan a transgredir las leyes, la misma Constitución y en concreto el libre funcionamiento de las telecomunicaciones. No sabemos las intenciones reales de sus posibles actos, pero sí las consecuencias que generarían dentro de una sociedad, o dentro de una persona en específico.

5.- MATERIALES Y METODOS

Durante el desarrollo de esta tesis, se aplicó el método científico que permitió tener conocimiento del problema objeto de estudio y posibilitó el planteamiento de una solución alternativa al mismo.

Se aplicaron además los métodos inductivo y deductivo, que permitieron partir de un conocimiento general, para ir a lo particular e identificar la factibilidad de contemplar la falsificación electrónica de instrumentos privados y públicos, empleando medios electrónicos, como delito informático.

Los datos obtenidos en el proceso de investigación fueron sometidos a los métodos analítico – sintético a través de los que se procedió a sistematizar la información teórica lograda para el análisis correspondiente.

La investigación fue de tipo documental y de campo. Como técnicas de investigación se aplicaron las siguientes: la observación, que durante el proceso investigativo constituyó una técnica que posibilitó el acercamiento directo del investigador con el problema planteado, tomando contacto con los protagonistas del mismo; se elaboraron fichas

bibliográficas, fichas mnemotécnicas, fichas de transcripción, para recolectar los elementos teórico doctrinarios que permitieron ilustrarnos respecto a la temática planteada y que constituyeron luego el fundamento de la sugerencia de las alternativas de solución; así también se elaboraron las fichas documentales correspondientes; se aplicaron cuarenta encuestas a abogados entre magistrados, jueces, agentes fiscales y profesionales del derecho en libre ejercicio, en el distrito judicial de Loja.

Los datos así recopilados fueron ordenados sistemáticamente para el análisis pertinente y constituyeron el fundamento para la redacción del informe final y el proyecto de reformas al Código Penal que propongo.

6.- RESULTADOS

Concluida la aplicación de las encuestas, mismas que cumpliendo con lo establecido en el proyecto de investigación se dirigieron a cuarenta profesionales, entre Magistrados, Jueces, Fiscales y Abogados en libre ejercicio, procedí a la tabulación de las respuestas y la interpretación de los resultados se realizó de manera cuantitativa y cualitativa.

PREGUNTA No. 1

1.- ¿Considera usted que los delitos cometidos a través de medios informáticos son importantes en nuestro país?

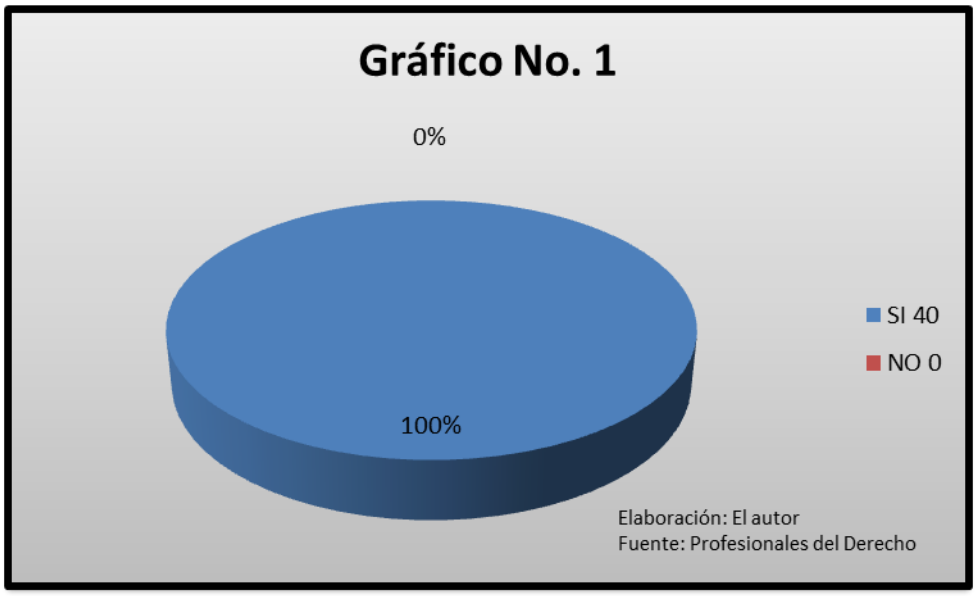
Si ( )

No ( )

CUADRO No. 1

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	40	100%
NO	0	0%
TOTAL	40	100%

Elaboración: El autor
Fuente: Profesionales del Derecho



Elaboración: El autor
Fuente: Profesionales del Derecho

INTERPRETACION

A esta interrogante 40 personas que representan el 100% del universo encuestado, responden de manera afirmativa, señalando que los delitos que se comenten a través de medios electrónicos o informáticos en nuestro país, tienen el carácter de importantes.

Los primeros tipos penales informáticos que se incluyeron en nuestra legislación fueron en el año 2002 con la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

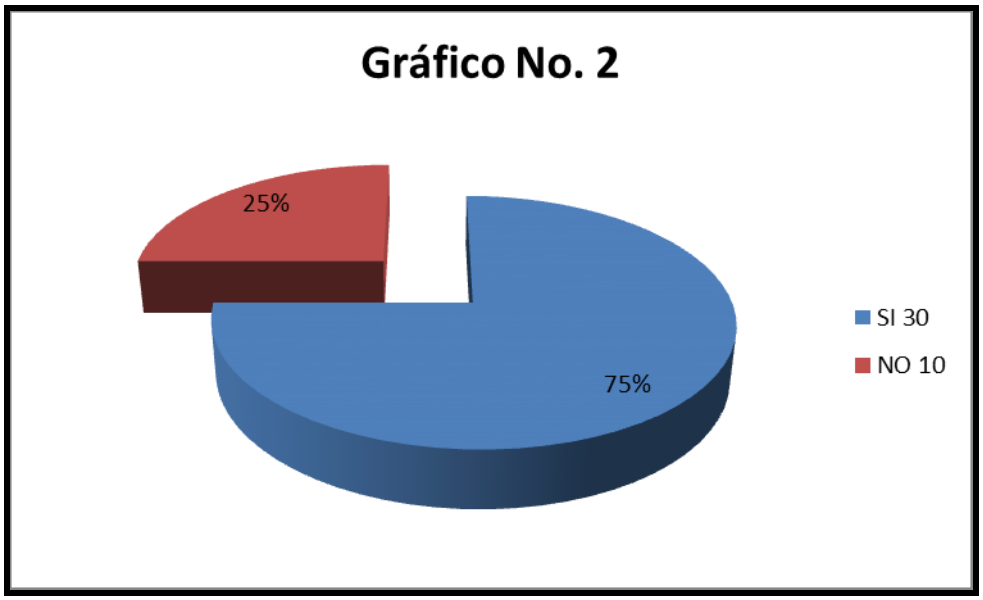
PREGUNTA No. 2

2.- Está usted de acuerdo en que los delitos informáticos están revestidos de algunos elementos constitutivos como dolo y sujeto activo cualificado?

CUADRO No. 2

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SI	30	75%
NO	10	25%
TOTAL	40	100%

Elaboración: El autor
Fuente: Profesionales del Derecho



Elaboración: El autor
Fuente: Profesionales del Derecho

INTERPRETACIÓN

Treinta profesionales que representan el setenta y cinco por ciento del universo encuestado, señalan que los delitos informáticos tienen como principales elementos constitutivos al dolo, el sujeto activo cualificado; criterio con el cual coincido, pues para perpetrar un delito de esta naturaleza se requiere tener conocimiento previo y además bastos conocimientos en informática.

PREGUNTA No. 3

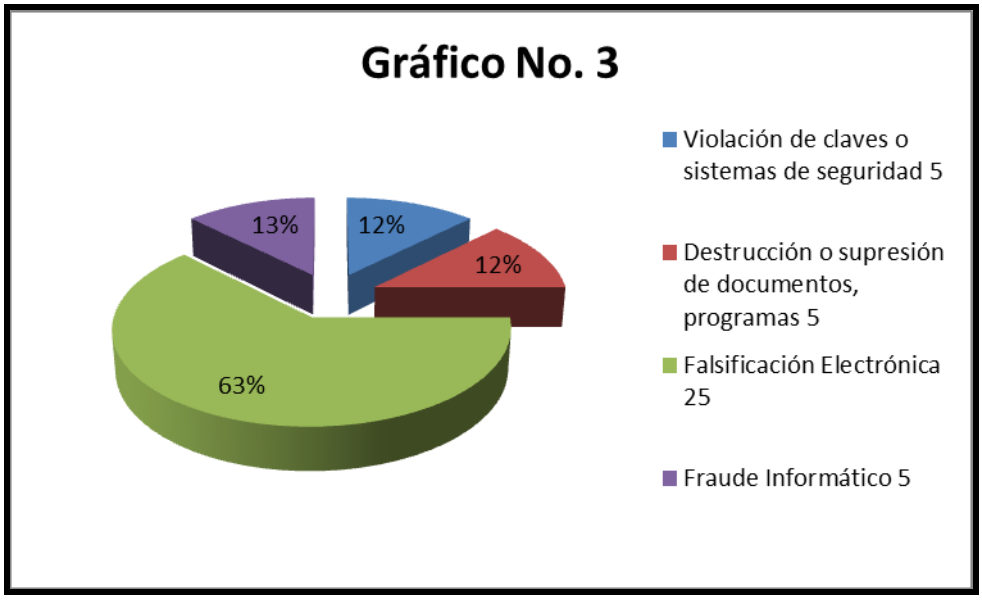
3.- Según su experiencia profesional, de los siguientes delitos considerados como informáticos, cual es el que con mayor frecuencia se denuncia:

- Violación de claves o sistemas de seguridad
- Destrucción o supresión de documentos, programas.
- Falsificación Electrónica
- Fraude Informático

CUADRO No. 3

ALTERNATIVA	FRECUENCIA	PORCENTAJE
VIOLACIÓN DE CLAVES O SISTEMAS DE SEGURIDAD	5	12.5%
DESTRUCCIÓN O SUPRESIÓN DE DOCUMENTOS, PROGRAMAS	5	12.5%
FALSIFICACIÓN ELECTRÓNICA	25	62.5%
FRAUDE INFORMÁTICO	5	12.5%
TOTAL	40	100%

Elaboración: El autor
Fuente: Profesionales del Derecho



Elaboración: El autor
Fuente: Profesionales del Derecho

INTERPRETACIÓN

De los cuarenta encuestados, cinco que corresponden al 12,5% del universo, señalan que el delito informático que con mayor frecuencia se denuncia es el de violación de claves o sistemas de seguridad; mientras que así mismo cinco encuestados que igualmente representan el 12,5% de personas, señalan que es la destrucción o supresión de documentos o programas, el que en mayor índice se denuncia; mientras que veinticinco personas que representan el 62,5% del universo encuestado, señalan que es la falsificación electrónica, el delito mayormente denunciado por la ciudadanía; y, finalmente cinco personas que representan también el 12,5% indican que es el fraude informático el delito informático que mayormente se comete y en consecuencia el mas denunciado.

Personalmente me sumo al criterio de la mayoría de los profesionales encuestados, pues es la falsificación electrónica el delito de moda en nuestro país. A diario escuchamos en medios de comunicación como personas desaprensivas hacen uso de su ingenio para sustraer datos de tarjetas de crédito, débito, etc., para posteriormente con esa información falsificar estos instrumentos y emplearlos en beneficio personal.

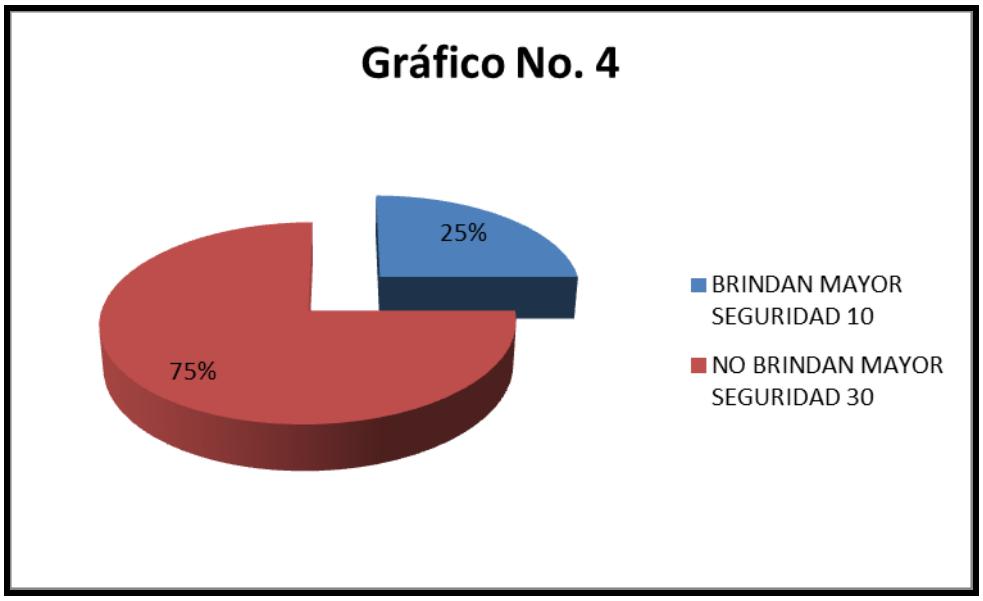
PREGUNTA No. 4

4.- ¿Diría usted que las transacciones efectuadas mediante medios electrónicos brindan más seguridad que las realizadas por medios convencionales?

CUADRO No. 4

ALTERNATIVA	FRECUENCIA	PORCENTAJE
BRINDAN MAYOR SEGURIDAD	10	25%
NO BRINDAN MAYOR SEGURIDAD	30	75%
TOTAL	40	100%

Elaboración: El autor
Fuente: Profesionales del Derecho



Elaboración: El autor
Fuente: Profesionales del Derecho

INTERPRETACIÓN

De las cuarenta personas encuestadas, diez que corresponden al 25% del universo, señalan que las transacciones efectuadas mediante medio electrónicos brindan mayor seguridad que las realizadas convencionalmente; mientras que treinta profesionales, que representan el 75% indican que este tipo de transacciones no brindan mayores seguridades que las que ofrece una transacción convencional.

Al criterio de la mayoría de personas me sumo, pues considero que el medio que se elija para efectuar una transacción, no es el problema, pues siempre estaremos expuestos a que alguna persona de mala fe perjudique a otro empleando cualquier artimaña. Considero que el problema es la corrupción que está enraizada en nuestra sociedad; pero mientras existan más medios electrónicos a través de los cuales se realicen toda clase de transacciones, nuestras leyes deben garantizar nuestros derechos e ir a la par de los adelantos tecnológicos para precautelarlos.

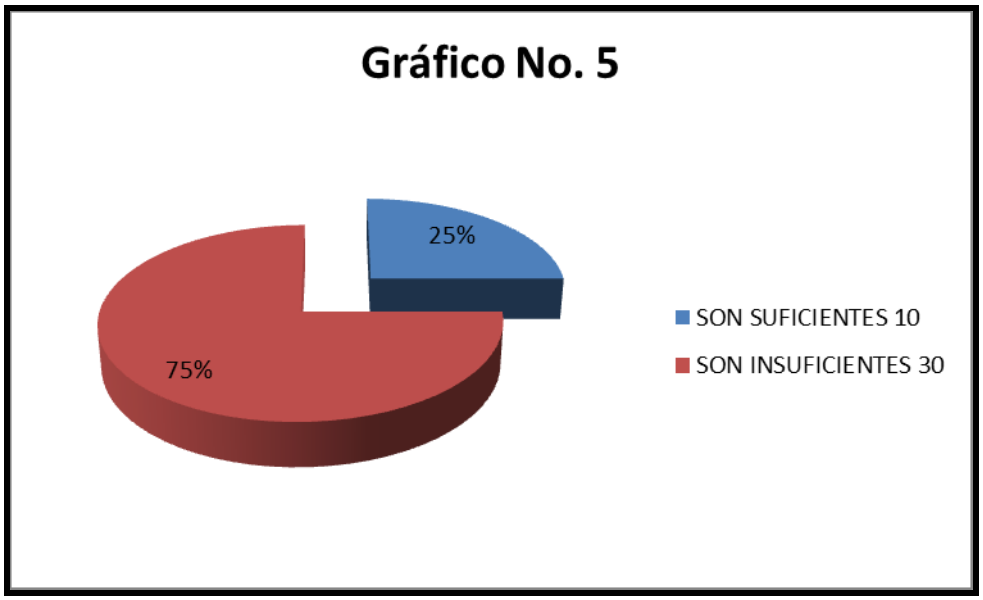
PREGUNTA No. 5

5.- Considera usted que las disposiciones legales que regulan la falsificación electrónica en nuestro medio, son suficientes?

CUADRO No. 5

ALTERNATIVA	FRECUENCIA	PORCENTAJE
SON SUFICIENTES	10	25%
SON INSUFICIENTES	30	75%
TOTAL	40	100%

Elaboración: El autor
Fuente: Profesionales del Derecho



INTERPRETACIÓN

Diez profesionales que representan el 25% del universo encuestado, señalan que las normas legales que actualmente contempla el Código Penal ecuatoriano, en relación a la tipificación y sanción de los delitos informáticos, específicamente la falsificación informática, son insuficientes; mientras que treinta encuestados que representan el 75%,

señalan que nuestra legislación es insuficientes para regular la falsificación electrónica; criterio del cual comparto, pues ante el importante aumento y la rápida evolución de los delitos informáticos, las leyes deben irse reformando para que contribuyan de mejor manera a lograr el objetivo de investigar y combatir los delitos relacionados con internet y las nuevas tecnologías.

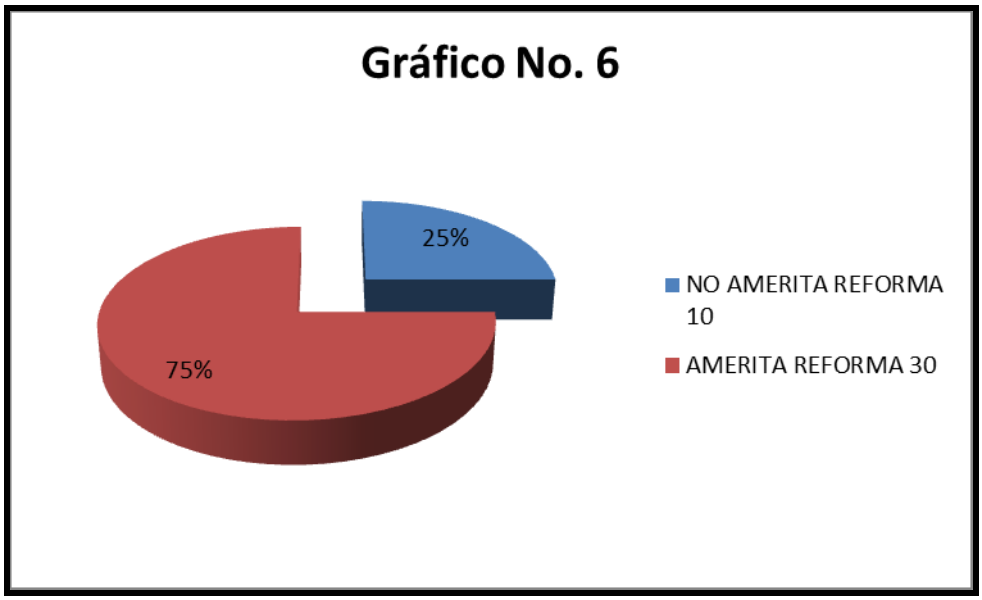
PREGUNTA No. 6

6.- Considera usted que el Código Penal ecuatoriano amerita una reforma a fin de incluir la falsificación de instrumentos públicos como delito informático?

CUADRO No. 6

ALTERNATIVA	FRECUENCIA	PORCENTAJE
AMERITA REFORMA	30	75%
NO AMERITA REFORMA	10	25%
TOTAL	40	100%

Elaboración: El autor
Fuente: Profesionales del Derecho



INTERPRETACIÓN

Treinta profesionales de los cuarenta encuestados, que representan el 75%, señalan que nuestro Código Penal amerita ser reformado a fin de incluir la falsificación de instrumentos públicos como delito informático; mientras que diez encuestados que representan el 25%, mencionan que no es necesaria ninguna clase de reforma al Código.

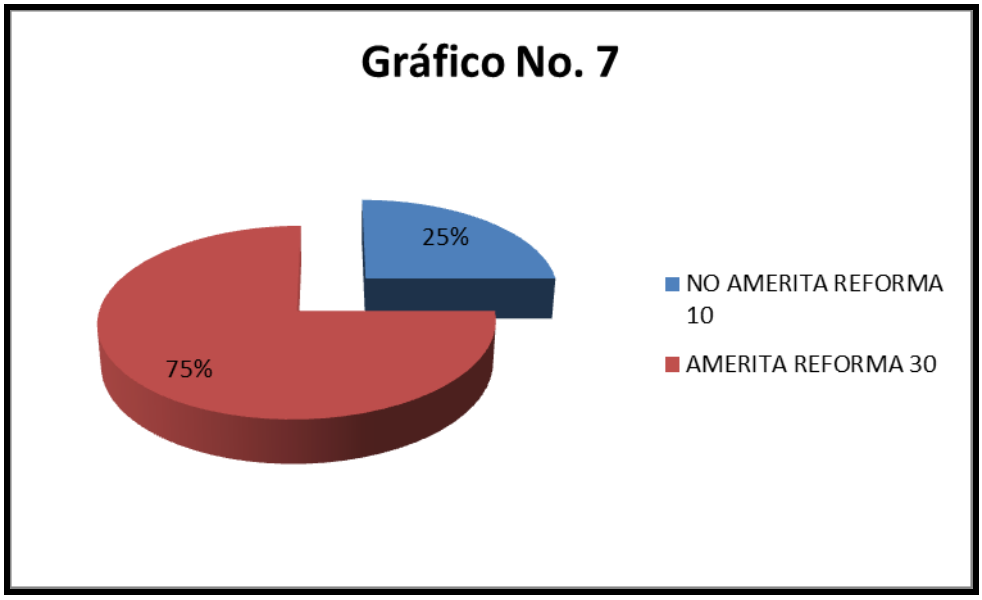
PREGUNTA No. 7

7.- Considera usted que el Código Penal ecuatoriano amerita una reforma a fin de incluir la falsificación de instrumentos privados como delito informático?

CUADRO No. 7

ALTERNATIVA	FRECUENCIA	PORCENTAJE
AMERITA REFORMA	30	75%
NO AMERITA REFORMA	10	25%
TOTAL	40	100%

Elaboración: El autor
Fuente: Profesionales del Derecho



INTERPRETACIÓN

Treinta profesionales de los cuarenta encuestados, que representan el 75%, señalan que nuestro Código Penal amerita ser reformado a fin de

incluir la falsificación de instrumentos públicos como delito informático; mientras que diez encuestados que representan el 25%, mencionan que no es necesaria ninguna clase de reforma al Código.

7.- DISCUSIÓN

Sustentación de la Problemática

Se ha efectuado y realizado un estudio analítico, jurídico y doctrinario a través de las diferentes teorías, conceptos, definiciones en relación con los delitos informáticos, en especial la falsificación informática, lo cual han sido destacado permanentemente a lo largo de este trabajo de investigación socio-jurídica, donde se emplearon los medios necesarios para llegar a determinar la necesidad de reformar su tipificación en la legislación penal.

Gracias a la colaboración de aquellas personas vinculadas y conocedores de la situación jurídica actual y una vez realizados los análisis de los diversos criterios que respondieron claramente las distintas preguntas planteadas en la encuesta, se puede concluir y sustentar que, en su mayoría, afirman que debe incorporarse en nuestro ordenamiento penal nuevas figuras que tipifiquen primordialmente la falsificación por medios electrónicos de instrumentos públicos y privados.

Verificación de Objetivos

En el proyecto de investigación jurídica se plantearon los siguientes objetivos:

Objetivo General

Realizar un estudio analítico de la normativa del Código Penal, que regula las clases, tipos penales y las respectivas sanciones sobre los delitos informáticos y la falsificación informática.

Este objetivo se verificó durante el desarrollo del trabajo investigativo, primordialmente con la revisión de literatura, en donde se detalló y analizó las disposiciones de nuestro Código Penal que regulan las conductas informáticas.

Objetivos Específicos

Demostrar que en la actualidad, existen casos de delitos y falsificación informática, que no tienen un tratamiento legal para ser juzgados.

Determinar que las disposiciones, en cuanto a las sanciones, no compaginan con la gravedad de los delitos informáticos y la falsificación informática en el Código Penal.

Este objetivo específico se verificó con el análisis efectuado a las disposiciones pertinentes del Código Penal y mediante la aplicación de la encuesta; en donde la mayoría de los profesionales del derecho indicaron que las sanciones que actualmente dispone el Código Penal son

insuficientes frente a la gravedad de las infracciones cometidas, esto tratándose de delitos como la falsificación informática.

Demostrar que la mayoría de ciudadanos, desconocen el tema de los delitos informáticos, la falsificación informática y si existe o no una normativa vigente que los regule y sancione.

Este objetivo específico al igual que el anterior se verificó mediante la aplicación de la encuesta, pues la mayoría de las respuestas dadas por los encuestados, se definen por una necesaria reforma al Código Penal que contemple algunas figuras jurídicas referentes a la falsificación informática de instrumentos públicos y privados.

Elaborar una propuesta de reforma al Código Penal, en el aspecto en que los sus vacíos legales, sean llenados para regular los delitos informáticos y la falsificación informática.

Objetivo que se verificó con la presentación del proyecto de reformas al Código Penal que como recomendación se adjunta en este informe de tesis.

Contrastación de Hipótesis

La **hipótesis** planteada en mi proyecto de tesis refería:

Las disposiciones tipificadas sobre los delitos informáticos y la falsificación informática en el Código Penal, contienen sanciones que no se enmarcan con la realidad y el peligro de estos delitos, propiciando así la impunidad.

La hipótesis fue contrastada con todo el estudio realizado y se ha demostrado afirmativamente, pues las sanciones que establece el Código Penal referentes a los delitos informáticos, específicamente la falsificación informática, resultan insuficientes, opinión que es compartida por la mayor parte de los profesionales que fueron encuestados y cuyas opiniones han sido plasmadas en el presente trabajo, y fueron de suma importancia porque de esta manera se pudo comprobar que existe un marco jurídico insuficiente para sancionar la falsificación informática.

8.- CONCLUSIONES

- La Informática tiene gran significancia y amplitud en la actualidad, puesto que abarca varios campos de las actividades que el ser humano realiza constantemente, sea en el ámbito educativo, profesional, laboral, financiero, administrativo, etc.

- Como ya lo mencionamos dentro del Delito, una de sus categorizaciones está el Delito Informático, y asimismo dentro de la definición lo que agregaríamos es, que esa acción se encamina al cometimiento de conductas inadecuadas con el uso o en contra de elementos informáticos (hardware y/o software).

- El tema de la delincuencia informática, no ha tenido la suficiente difusión en la ciudadanía, razón por lo cual la mayor parte de la población no posee ni siquiera un conocimiento básico de su incidencia en la actualidad.

- Se reconoce que casi la mayoría de la clasificación de delitos informáticos, son difíciles de perseguir por cuanto, por las cualidades del sujeto activo de este tipo de infracciones, las

huellas de los mismos son borradas con cierta facilidad, evadiendo las investigaciones y controles de las autoridades.

- La carencia de cultura informática en nuestra sociedad, es un elemento crítico en el impacto de los delitos informáticos, cada día se requieren mayores conocimientos en tecnologías de la información, que permitan manejar estas situaciones.

- Existen dentro de la sociedad un sinnúmero de delitos informáticos, unos más perpetrados que otros, unos más conocidos que otros, pero la mayoría de delitos informáticos, son difíciles de perseguir por cuanto, las huellas de los mismos son borradas con cierta facilidad, evadiendo las investigaciones y controles de las autoridades.

- Las personas, instituciones u organizaciones que se vieran afectadas por la presencia de delitos informáticos, no debe impedir o dejar de lado los beneficios de todo lo que proveen las tecnologías de información, más bien por el contrario dicha situación debe tomarse como un reto, de manera que se realicen esfuerzos encaminados a robustecer los aspectos de seguridad,

controles, integridad de la información, etc., en los sistemas informáticos.

- Si bien se ha intentado controlar los delitos informáticos, tipificando y sancionando estas conductas inadecuadas, seguimos siendo vulnerables a estas infracciones. Más aún la carencia de control, hace del mundo de la Informática y la Telemática, un lugar sin fronteras, donde prácticamente los gobiernos del mundo, no lo pueden regir.

- Uno de los delitos informáticos, conocidos y consumados en nuestro país, es la Falsificación Informática, una conducta dirigida a la adulteración, cambio, modificación de datos, archivos, sistemas de entidades públicas o privadas, y en fin todo tipo de documento, con la ayuda de programas o simplemente con la intervención fácil del hombre para alterar el correcto funcionamiento de un computador, pudiendo efectuársela tanto en instrumentos Públicos como Privados, dentro de los cuales se destacan las tarjetas de crédito y débito.

- Bien es cierto, que los delitos informáticos, llegan a violar un derecho que la misma Constitución de la República consagra y este

es el derecho a la intimidad o privacidad personal. Puesto que al ser objeto de cualquiera de estos delitos, somos afectados en nuestra reserva, y lo que es más importante, nuestra libertad en poseer datos, archivos personales, documentos públicos y privados, informes contenida en entidades públicas acerca de nuestros antecedentes, bienes, propiedades, etc. En síntesis toda la información correspondiente a un individuo en particular, por ende su divulgación no está permitida, a no ser por orden judicial.

- En el tema de la falsificación informática, no se sanciona con una normativa clara y específica a los autores, cómplices y encubridores de este delito, se allana a mencionar que serán sancionados de acuerdo a lo dispuesto en este capítulo, esto no se puede concebir. Y aún más, el contenido es insuficiente, no abarca todo lo que comprende esta infracción.

- Nuestro país aún es vulnerable ante la presencia de esta clase de delitos, peor cuando no existe control, haciedo del mundo de la Informática y la Telemática, un lugar sin fronteras, donde prácticamente los gobiernos del mundo, no lo pueden regir, nadie tiene reglas, nadie sabe lo que hace.

9.- RECOMENDACIONES

- Que la administración de la Justicia se mantenga a la vanguardia en tecnologías, técnicas y procedimientos, a fin de combatir adecuadamente esta tipo de ilícitos.

- Que las Universidades e Instituciones Tecnológicas Superiores tanto en carreras como Derecho o Sistemas deben incluir en su malla curricular el tema de los delitos informáticos y las formas de prevención.

- Que el Estado proporcione a la comunidad, la información necesaria a través de los medios de comunicación y otros medios de información sobre los distintos tipos de delitos informáticos que existe, su origen, causas, consecuencias de estos ilícitos.

- Que los operadores de justicia durante la investigación preprocesal y procesal penal tratándose de delitos informáticos se rijan de acuerdo a las recomendaciones que en el presente trabajo investigativo se ha realizado, concretamente en el punto con lo cual espero generar un aporte significativo a la administración de justicia de nuestro país.

- Que es necesario incorporar en el Código Penal, un capítulo específicamente destinado a estipular los diferentes ilícitos informáticos como por ejemplo: Falsificación Informática de Instrumentos Públicos y Privados, Superzap, Manipulación indebida de datos, Caballo de Troya, Técnica de Salami, Intervención o pinchado de las líneas de comunicación, Sabotaje informático, Piratería informática, Gusanos, Bombas lógicas, Hacking, Lectura e intervención en un email, Fraudes informáticos, Transferencia informática ilegal de fondos, Spamming, Espionaje Informático, Fishing, Pharming, Skimming, entre otros, por lo cual me permito presentar el siguiente proyecto de reformas al Código Sustantivo Penal:

9.1. PROPUESTA DE REFORMAS AL CODIGO PENAL ECUATORIANO

LA HONORABLE ASAMBLEA NACIONAL

DE LA REPUBLICA DEL ECUADOR

CONSIDERANDO

Que, la Constitución de la República del Ecuador en su Art. 3 preceptúa como deber primordial del Estado el garantizar a sus habitantes el derecho a una cultura de paz, a la seguridad integral y a vivir en una sociedad democrática y libre de corrupción;

Que la Carta Magna en su artículo 66 reconoce y garantizará a las personas, entre otros el derecho a la integridad personal, que incluye la integridad física, psíquica, moral y sexual;

Que la Constitución de la República del Ecuador, al referirse a la seguridad humana, establece en su artículo 393 que el Estado garantizará la seguridad humana a través de políticas y acciones integradas, para asegurar la convivencia pacífica de las personas, promover una cultura de paz y prevenir las formas de violencia y discriminación y la comisión de infracciones y delitos;

Que en el numeral 9 del artículo 11 del texto constitucional se establece como más alto deber del Estado el respetar y hacer respetar los derechos garantizados en la Constitución;

Que en el artículo 424 del texto constitucional, se establece la supremacía que tiene la Constitución sobre cualquier otra norma del ordenamiento jurídico;

Que es necesario, plantar reformas dentro de los Delitos Informáticos existentes en el Código Penal, en especial de la Falsificación Informática, por lo que a continuación planteo las siguientes:

Que es necesario agregar incisos, numerales para señalar tanto a la falsificación informática de instrumentos públicos, como la falsificación informática de instrumentos privados.

Que la Constitución de la República del Ecuador, en el numeral 6 del artículo 120, preceptúa entre las atribuciones y deberes de la Asamblea Nacional, el expedir, codificar, reformar y derogar las leyes e interpretarlas con carácter generalmente obligatorio;

En uso de sus atribuciones, resuelve expedir la siguiente:

LEY REFORMATORIA AL CÓDIGO PENAL DEL ECUADOR

ARTÍCULO PRIMERO.- Luego del artículo 353.1, agréguese un artículo que dirá: ….353.2 Falsificación Informática de Instrumentos Públicos.- Será reprimido con reclusión menor ordinaria de seis a nueve años, el que hubiere adulterado, cambiado o modificado un instrumento o documento público a través de un medio, programa o sistema informático. Igual pena se aplicará al titular de tal instrumento, que hubiese consentido tal alteración.

Los servidores públicos, estando o no en el ejercicio de sus funciones cometieren este delito, serán sancionados con una pena de reclusión menor extraordinaria de nueve a doce años, y la correspondiente destitución e inhabilitación para el desempeño de un cargo público.

ARTÍCULO SEGUNDO.- Agréguese a continuación un artículo que dirá: ...353.3 Falsificación Informática de Instrumentos Privados.- Será reprimido con reclusión menor ordinaria de seis a nueve años, el que hubiere falsificado, alterado, cambiado o modificado un instrumento o documento privado, entendido como este a las tarjetas de crédito y débito a través de un medio, programa o sistema informático.

Quienes maliciosamente a través de la falsificación informática, obtengan beneficios económicos con el uso de las tarjetas de crédito o débito a las que se hace referencia en el inciso anterior, además de la pena impuesta, están obligados a pagar el monto del perjuicio ocasionado al titular de la misma, así como la multa de quinientos a mil dólares de los Estados Unidos de América.

El funcionario público o empleado privado, encargados del manejo y custodia del sistema informático de la entidad correspondiente, que participare en el cometimiento de esta infracción, serán sancionados con reclusión menor extraordinaria de nueve a doce años, quedando además obligados a pagar el monto del perjuicio ocasionado al titular, en caso de no habérselo efectuado conforme la disposición del inciso anterior y la correspondiente destitución e inhabilitación para el desempeño de un cargo público.

10.- BIBLIOGRAFÍA

1. ALULEMA MEDINA, Ricardo Javier. Guía para la Recolección de Evidencia Digital en el Ecuador. Pontificia Universidad Católica del Ecuador, Facultad de Ingeniería. Quito. 2008.

2. ÁLVAREZ MARAÑON, Gonzalo. Seguridad Informática para Empresas y Particulares. McGraw-Hill. Madrid España. 2004.

3. CABANELLAS DE LAS CUEVAS, Guillermo. Derecho de Internet/ comp. Heliasta. Buenos Aires, Argentina. 2004.

4. CONWAY, James V.P. Evidencias documentales. Ediciones La Rocca. Buenos Aires, Argentina.

5. CREUS, Carlos, BUOMPADRE, Jorge. Falsificación de Documentos en General. Editorial ASTREA. Buenos Aires, Argentina. 1986.

6. DÍAZ GARCÍA, Alexander. Derecho Informático. Elementos de la Informática Jurídica. Leyer. Bogotá, Colombia. 2002.

7. GÁLLEGO HIGUERAS, Gonzalo. Código de Derecho Informático y de las Nuevas Tecnologías. Editorial Civitas. Madrid España. 2003.

8. GONZÁLEZ, Jorge. Documentología: Estudio del Documento Dudoso y su Aplicación en el Ámbito Judicial Ecuatoriano. Gráficas San Rafael. Ecuador. 2008.

9. GUIBOURG, Ricard; Aliende, Jorge; Campanella, Elena A. Manual de Informática Jurídica. Astrea. Buenos Aires, Argentina. 1996.

10. HERBERTSON, Gary. Examen del Documento en la Computadora. Ediciones
la Rocca. Buenos Aires, Argentina. 2004.

11. JIJENA LEIVA, Renato Javier. Comercio Electrónico. Editorial Andrés Bello. Santiago de Chile, Chile. 2002.

12. MÁRQUEZ ESCOBAR, Carlos Pablo. El Delito Informático conforme con el nuevo Código Penal: la Información y la Comunicación en la Esfera Penal. Leyer. Bogotá, Colombia. 2002.

13. MANERA, Alberto E. Falsedades Documentales por Computadora. Ediciones La Rocca. FALSIFICACIÓN DE DOCUMENTOS. Buenos Aires, Argentina. 2006.

14. RIELO, Antonio. El Sistema Telemático. Lex net. España. 2006.

15. ROLDÁN, Patricio R. Documentación Pericial Caligráfica. Ediciones La Rocca. Buenos Aires, Argentina. 2006.

16. ROVIRA DEL CANTO, Enrique. Delincuencia Informática y Fraudes Informáticos. Comares. Granada, España. 2002.

17. Ruptura 44. Por La Legalidad. Asociación Escuela de Derecho de la Pontificia Universidad Católica del Ecuador. Quito. 2001.

18. TÉLLEZ VALDÉZ, Julio. Derecho Informático. McGraw- Hill. Tercera Edición. México, México. 2003.

19. VÁZQUEZ, IRUZUBIETA, Carlos. Manual de Derecho Informático. Difusa. Madrid, España. 2002.

20. YÁNEZ N, Pablo. Introducción al Estudio del Derecho Informático e Informática Jurídica. Escuela Politécnica Javeriana del Ecuador. 1999.

21. EDICIONES LEGALES.- Constitución de la República del Ecuador

22. EDICIONES LEGALES.- Código Penal del Ecuador

23. EDICIONES LEGALES.- Código de Procedimiento Penal del Ecuador

24. EDICIONES LEGALES.- Código Civil del Ecuador

25. EDICIONES LEGALES.- Código de Procedimiento Civil

11. ANEXOS

FORMULARIO DE ENCUESTA

UNIVERSIDAD NACIONAL DE LOJA

MODALIDAD DE ESTUDIOS A DISTANCIA

CARRERA DE DERECHO

Señor Abogado, me dirijo a usted a través de la presente encuesta con la finalidad de solicitar se digne dar contestación a lo solicitado en la misma, en vista que me encuentro desarrollando mi trabajo de tesis previo a la obtención del título de Abogado, sobre el tema "INSUFICIENTE NORMATIVA EN EL CÓDIGO PENAL, SOBRE LOS DELITOS INFORMÁTICOS Y LA FALSIFICACIÓN INFORMÁTICA, EN CUANTO A LOS TIPOS PENALES Y LAS SANCIONES" y su criterio será de mucho valor para llevar adelante mi trabajo investigativo.

PREGUNTA No. 1

1.- ¿Considera usted que los delitos cometidos a través de medios informáticos son importantes en nuestro país?

Si ( )

No ( )

PREGUNTA No. 2

2.- Está usted de acuerdo en que los delitos informáticos están revestidos de algunos elementos constitutivos como dolo y sujeto activo cualificado?

Si ( )

No ( )

PREGUNTA No. 3

3.- Según su experiencia profesional, de los siguientes delitos considerados como informáticos, cual es el que con mayor frecuencia se denuncia:

- Violación de claves o sistemas de seguridad
- Destrucción o supresión de documentos, programas.
- Falsificación Electrónica
- Fraude Informático

PREGUNTA No. 4

4.- ¿Diría usted que las transacciones efectuadas mediante medios electrónicos brindan más seguridad que las realizadas por medios convencionales?

Si ( )

No ( )

PREGUNTA No. 5

5.- Considera usted que las disposiciones legales que regulan la falsificación electrónica en nuestro medio, son suficientes?

Si ( )

No ( )

PREGUNTA No. 6

6.- Considera usted que el Código Penal ecuatoriano amerita una reforma a fin de incluir la falsificación de instrumentos públicos como delito informático?

Si ( )

No ( )

PREGUNTA No. 7

7.- Considera usted que el Código Penal ecuatoriano amerita una reforma a fin de incluir la falsificación de instrumentos privados como delito informático?

Si ( )

No ( )

Gracias

INDICE