UNIVERSIDAD NACIONAL DE LOJA
MODALIDAD DE ESTUDIOS A DISTANCIA

CARRERA DE DERECHO

TEMA

"REFORMAS EN CUANTO A CASTIGAR SEVERAMENTE LAS INFRACCIONES INFORMÁTICAS EN LA LEGISLACIÓN PENAL ECUATORIANA"

TESIS PREVIO A LA OBTENCION DEL TITULO DE ABOGADO

POSTULANTE
Luis Pablo Méndez Vanegas

DIRECTOR
Dr. Mario Alfonso Guerrero González **Mg. Sc.**

LOJA-ECUADOR
2012

II. CERTIFICACIÓN DEL DIRECTOR

Dr. Mario Alfonso Guerrero González, Docente de la Carrera de Derecho de la Modalidad de Estudios a Distancia de la Universidad Nacional de Loja:

C E R T I F I C O:

Haber dirigido y revisado prolijamente en todas sus fases el trabajo de tesis previo a la obtención del tirulo de Abogado del postulante **LUIS PABLO MENDEZ VANEGAS**cuyo título es: **"REFORMAS EN CUANTO A CASTIGAR SEVERAMENTE LAS INFRACCIONES INFORMÁTICAS EN LA LEGISLACIÓN PENAL ECUATORIANA",** y en virtud de que cumple con los requisitos establecidos en el Reglamento de Régimen Académico, de la Universidad Nacional de Loja Autorizo su presentación y sustentación pública.

Loja, octubre de 2012.

Dr. Mario Alfonso Guerrero González. Mg. Sc.
DOCENTE CARRERA DE DERECHO
MODALIDAD DE ESTUDIOS A DISTANCIA
UNIVERSIDAD NACIONAL DE LOJA.

III. DECLARACIÒN DE AUTORÍA

Todos los comentarios, ideas, análisis y críticas sobre la información, presentada en el desarrollo del presente trabajo de Tesis denominado **“REFORMAS EN CUANTO A CASTIGAR SEVERAMENTE LAS INFRACCIONES INFORMÁTICAS EN LA LEGISLACIÓN PENAL ECUATORIANA”** son de mi exclusiva responsabilidad y autoría, asumiendo todas las responsabilidades que el caso amerite.

Loja, octubre de 2012

LUIS PABLO MENDEZ VANEGAS
POSTULANTE

IV. DEDICATORIA

El desarrollo de este trabajo lo dedico a todos mis familiares y amigos quienes me has sabido apoyar y dar ánimo para cumplir con éxito mi carrera profesional y sobre todo para el desarrollo del presente trabajo de tesis previo a la obtención del título de Abogado.

El Autor

V. AGRADECIMIENTO

Quiero expresar mis sinceros sentimientos de agradecimiento y gratitud a la Universidad Nacional de Loja, a sus Autoridades, a la Modalidad de Estudios a Distancia, a sus Autoridades, a los docentes de la Carrera de Derecho, de manera especial al señor Dr. Mario Alfonso Guerrero González, quien con su vocación de docente, y sobre todo con un don de gente, ha guiado de forma profesional y desinteresada el desarrollo del presente trabajo, digno de reconocimiento y admiración.

El Autor

VI. TABLA DE CONTENIDOS

1. TÍTULO

“REFORMAS EN CUANTO A CASTIGAR SEVERAMENTE LAS INFRACCIONES INFORMÁTICAS EN LA LEGISLACIÓN PENAL ECUATORIANA”

2. RESUMEN

El aspecto más importante de la informática es información, la cual ha llegado alcanzar un gran valor económico, el correcto uso de esta información, puede crear grandes redes de servicios, comercio, educación etc., apoyando al desarrollo de los pueblos. Desgraciadamente en todas las facetas de la actividad humana, existe el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva el delito, lo que ha permitido que los delincuentes se aprovechen de la vulnerabilidad del acceso de información a través de redes de comunicación cometiendo una serie de delitos informáticos, de índole patrimonial y socio-económico, produciendo innumerables perjuicios a las personas.

La Constitución de la República del Ecuador al referirse a los Derechos de libertad en su Art. 66 numerales 19 y 20 establece la protección de la información personal en todos sus aspectos, esta protección consta entre los derechos de libertad de las personas, es por ello que la información personal es considerada como confidencial y su acceso, divulgación y uso deben estar autorizados por el titular o por el mandato de la Ley, la violación a ello constituye un delito que podría causar daños irreparables.

En el Libro Segundo del Código Penal en el CAPITULO V, se refiere a los delitos contra la inviolabilidad del secreto, determinando en su Art. 202 A, que “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…",estableciendo además algunas circunstancias que agravan las sanciones, pero resultan leves para la gravedad de la infracción cometida, siendo necesario que se castigue severamente estas conductas.

Por todo lo anteriormente señalado, he creído conveniente realizar el presente trabajo de tesis orientado a la necesidad urgente de reformar en el Código Penal Ecuatoriano, el marco sancionador de las infracciones informáticas con el fin de frenar el auge de la delincuencia que cometen estos delitos.

2.1 ABSTRACT.

The most important aspect of computing is information which has come to achieve a high economic value, the proper use of this information; you can create large networks of services, trade, and education and so on, supporting the development of peoples. Unfortunately in all facets of human activity, there is deceit, manipulation, greed, lust for revenge, fraud in the end the offense, which has allowed criminals to take advantage of the vulnerability of access to information communication networks of committing a series of computer crime and socio-economic equity in nature, producing harm to countless people.

The Constitution of the Republic of Ecuador to refer to the laws of freedom in Article 66 paragraphs 19 and 20 provides for the protection of personal information in all its aspects, this protection includes the rights of personal freedom, which is why that personal information is considered confidential and access, dissemination and use must be authorized by the owner or the mandate of the Act, the violation is an offense it could cause irreparable damage.

In the Second Book of the Penal Code in Chapter V, refers to offenses against the sanctity of the secret, determining in its Article 202 A, which.

"He that using any means, electronic, computer or similar, violentare keys or security systems, to access or obtain protected information contained in information systems, to undermine the secrecy, confidentiality and discretion, or simply violate the security shall be punished with imprisonment for six months to a year and a fine of five hundred thousand dollars to the United States of America ... ", also establishing some circumstances that aggravate the penalties, but they are mild to the seriousness of the offense, being necessary to punish severely those behaviors.

For all the above, I have seen fit to make this thesis focused on the urgent need for reform in the Ecuadorian Criminal Code, under penalty of computer offenses in order to curb the rise in crime who commit these crimes.

3. INTRODUCCIÓN

El presente trabajo de Tesis, titulada **"REFORMAS EN CUANTO A CASTIGAR SEVERAMENTE LAS INFRACCIONES INFORMÁTICAS EN LA LEGISLACIÓN PENAL ECUATORIANA",** se constituye una amplia recopilación de información y análisis jurídico, crítico y doctrinario de las Infracciones Informáticas y su regulación en el Código Penal Ecuatoriano, el cual he desarrollado luego de haber cursado mis estudios universitarios en la carrera de Derecho, donde logré obtener grandes conocimiento y destrezas fundamentales para este tipo de trabajo.

Iniciando el trabajo estructuré el marco conceptual necesario para facilitar la comprensión de los lectores, aquí presento varias definiciones de términos de uso frecuente y rutinario, realizadas por diferentes autores los cuales considero fundamentales en el desarrollo de la presente Tesis; para luego realizar una exposición detallada de lo que varios autores han escrito en relación a la problemática planteada, lo que nos permite ampliar nuestro horizonte y nos da mayores elementos de juicio, para continuar realizando la presentación y análisis de la normativa jurídica que regula las infracciones informáticas, en la legislación ecuatoriana.

Continuando con el desarrollo del trabajo se presenta un análisis de diferentes legislaciones que hablan sobre las infracciones informáticas, lo que me permitió comparar las normas reguladoras de las infracciones

informáticas que se aplican en otras legislaciones, lo cual sin duda facilita la comprensión del presente trabajo.

Una vez recopilada toda la información pongo a su conocimiento los materiales y métodos utilizados para el desarrollo del presente trabajo, de esta manera se puede presentar de forma clara los resultados de la encuesta, con su representación gráfica, análisis cuantitativo y cualitativo.

Ya en la parte final de la presente tesis realizo la comprobación de los objetivos y la contratación de hipótesis, lo que nos permitió presentar las conclusiones y recomendaciones que surgen luego del presente trabajo, y la propuesta de reforma jurídica, el detalle de la bibliografía utilizada, así como los anexos del presente trabajo.

4. REVISION DE LITERATURA

Con el pasar del tiempo conforme la sociedad ha ido transformándose y evolucionando, la delincuencia y el crimen organizado no se han quedado atrás de esta evolución, ideándose nuevas formas para cometer sus ilícitos.

4.1. MARCO CONCEPTUAL

Es necesario citar algunos conceptos que facilitaran la comprensión del presente trabajo, es así que en primer lugar es factible determinar el significado de Infracción de la cual Guillermo Cabanellas manifiesta *"Transgresión, quebrantamiento, violación, incumplimiento de una ley, pacto o tratado."*[1], esta pequeña pero concreta definición nos permite conocer que una infracción no es otra cosa que actuar u obrar fuera o en contra de las leyes que rigen a determinado grupo de personas o naciones.

Si actuamos en contra de la Ley, estamos atentando de manera directa contra el resto de personas o sus bienes, determinado esto podemos manifestar que este quebrantamiento obviamente que debe ser ideado, planificado y ejecutado por personas, que se las conoce como Infractor, transgresor, delincuente.

[1] CABANELLAS, Guillermo, Diccionario Jurídico Elemental, Editorial Heliasta, Buenos Aires-Argentina.

Para cometer este tipo de actos delictivos las personas han utilizado la Tecnología sus conocimientos o una mezcla de ellos es así que para cumplir sus objetivos esto es aplicando por ejemplo aparatos electrónicos o informáticos como:

Computadores de escritorio o portátiles.

1. Servidores que almacenan o transfieren datos electrónicos por internet.
2. Teléfonos celulares.
3. Aparatos para identificar llamadas.
4. GPS, aparato que utiliza el satélite para ubicar a personas o vehículos.
5. Cámaras de Video.
6. Sistemas de Seguridad, etc.

Instrumentos que al parecer son inofensivos pero en el momento de que el crimen organizado hace uso de ellos de forma ilícita, pueden provocar severos daños y perjuicios a las personas.

La revisión literaria en relación a la temática planteada debo traer a colación varias definiciones, que brindaran su aporte para una mejor comprensión del presente trabajo de investigación jurídica.

El centro del presente trabajo son las infracciones informáticas, las cuales son definidas por:

"*la realización de una acción que, reuniendo las características que delimitan el concepto de delito, sea llevada a cabo utilizando un elemento informático y/o telemático, o vulnerando los derechos del titular de un elemento informático, ya sea hardwareo software."*[2],

Esta definición le da una característica al acto desarrollado al margen de la ley, por su forma de materializarlo, esto es, utilizando medios tecnológicos electrónicos o informáticos, agregando que estos pueden ser de tipo hardware o software.

Las palabras hardware o software para muchos de los lectores serán familiares, pero para otros a lo mejor sean palabras nuevas, es por ello que me permitiré presentar una breve definición de estas.

En la Enciclopedia libre Wikipedia podes encontrar una definición precisa para Hardware donde se señala:

¨corresponde a todas las partes tangibles de un sistema informático: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado. El término es propio del idioma inglés (literalmente traducido: partes duras), su traducción al español no tiene un significado

[2]**DAVARA RODRÍGUEZ, Miguel Ángel,** Análisis de la Ley de Fraude Informático, Revista de Derecho de UNAM. 1990.

acorde, por tal motivo se la ha adoptado tal cual es y suena; la Real Academia Española lo define como Conjunto de los componentes que integran la parte material de una computadora¨.[3]

Esta definición nos permite comprender que el hardware, es toda la parte física, percibible y palpable por los individuos, de los diferentes equipos o aparatos electrónicos de diferentes usos y aplicaciones.

Al contrario Software es ¨e*l equipamiento lógico o soporte lógico* de un sistema informático; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos, que son llamados hardware.¨[4]

Este componente es la parte lógica, ficticia, que permite desarrollar una serie de actividades, que para su correcto funcionamiento deben existir los dos elementos el Hardware y el Software.

Hay definiciones mucho más complejas como la realizada por Julio Téllez Valdés quien conceptualiza al delito informático en forma típica y atípica, como: *"las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin; y, actitudes ilícitas en que se tienen a las computadoras como instrumento o fin"5.*

[3]WIKIPEDIA. http://es.wikipedia.org/wiki/Hardware.07/11/2011.
[4] Ibídem. http://es.wikipedia.org/wiki/Software.07/11/2011.
[5]**TELLEZ VALDÉS, Julio.** "Los Delitos informáticos. Situación en México",Informática y Derecho Nº 9, 10 y 11, UNED, Centro Regional de Extremadura,Mérida, 1996.

Otras definiciones como:

4.1.1 Internet.-

"*Es un conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial. Sus orígenes se remontan a 1969, cuando se estableció la primera conexión de computadoras, conocida como ARPANET, entre tres universidades en California y una en Utah, Estados Unidos."*[6].

En conclusión, Internet es tanto un conjunto de comunidades como un conjunto de tecnologías, y su éxito se puede atribuir a la satisfacción de las necesidades básicas de la comunidad y a la utilización de ésta de un modo efectivo para impulsar la infraestructura. Es a la vez una oportunidad de difusión mundial, un mecanismo de propagación de la información y un medio de colaboración e interacción entre los individuos y sus ordenadores, independientemente de su localización geográfica.

4.1.2. Los fraudes.-

"*Los Datos Falsos o Engañosos (Data diddling), conocido también como introducción de datos falsos, es una manipulación de datos de entrada al computador con el fin de producir o lograr movimientos falsos en transacciones de una empresa. Este tipo de fraude informático conocido también como manipulación de datos de entrada, representa el delito informático más común ya que es fácil de cometer y difícil de descubrir"*[7].

[6]WIKIPEDIA. http://es.wikipedia.org/wiki/Internet.07/11/2011
[7]ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador

Debo indicar que en este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.

4.1.3. Manipulación de Programas o Los "Caballos de Troya" (Troya Horses).-

"*Es muy difícil de descubrir y a menudo pasa inadvertida debido a que el delincuente debe tener conocimientos técnicos concretos de informática. Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o nuevas rutinas*"[8].

Este es un método común utilizado por las personas que tienen conocimientos especializados en programación informática es el denominado Caballo de Troya que consiste en insertar instrucciones de computadora de forma encubierta en un programa informático para que pueda realizar una función no autorizada al mismo tiempo que su función normal.

4.1.4 La técnica del salami (Salami Technique/Rounching Down).-

"*Aprovecha las repeticiones automáticas de los procesos de cómputo. Es una técnica especializada que se denomina "técnica del salchichón" en la que "rodajas muy finas" apenas perceptibles, de transacciones financieras, se*

[8]ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador

van sacando repetidamente de una cuenta y se transfieren a otra. Y consiste en introducir al programa unas instrucciones para que remita a una determinada cuenta los céntimos de dinero de muchas cuentas corrientes"[9].

4.1.5. Falsificaciones informáticas:

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

Como instrumentos*: Las computadoras pueden utilizarse también para efectuar falsificaciones de documentos de uso comercial. Cuando empezó a disponerse de fotocopiadoras computarizadas en color basándose en rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas"*[10].

Estas fotocopiadoras pueden hacer reproducciones de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.

4.1.6. Manipulación de los datos de salida.-

"*Se efectúa fijando un objetivo al funcionamiento del sistema informático. El ejemplo más común es el fraude de que se hace objeto a los cajeros automáticos mediante la falsificación de instrucciones para la computadora*

[9] ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador
[10] ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador

en la fase de adquisición de datos. Tradicionalmente esos fraudes se hacían basándose en tarjetas bancarias robada"[11].

Sin embargo, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.

4.1.7. Pishing.-

"*Es una modalidad de fraude informático diseñada con la finalidad de robarle la identidad al sujeto pasivo. El delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o de ventanas emergentes. El robo de identidad es uno de los delitos que más ha aumentado. La mayoría de las víctimas son golpeadas con secuestros de cuentas de tarjetas de crédito, pero para muchas otras la situación es aún peor"*[12].

En los últimos cinco años 10 millones de personas han sido víctimas de delincuentes que han abierto cuentas de tarjetas de crédito o con empresas de servicio público, o que han solicitado hipotecas con el nombre de las víctimas, todo lo cual ha ocasionado una red fraudulenta que tardará años en poderse desenmarañar. En estos momentos también existe una nueva modalidad de Pishing que es el llamado SpearPishing o Pishing

[11] ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador
[12] ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador

segmentado, el cual ataca a grupos determinados, es decir se busca grupos de personas vulnerables a diferencia de la modalidad anterior.

4.1.8. El sabotaje informático.-Es el acto de borrar, suprimir o modificar sin autorización funciones o datos de computadora con intención de obstaculizar el funcionamiento normal del sistema. Las técnicas que permiten cometer sabotajes informáticos son:

4.1.9. Bombas lógicas (LogicBombs).-

"Es una especie de bomba de tiempo que debe producir daños posteriormente. Exige conocimientos especializados ya que requiere la programación de la destrucción o modificación de datos en un momento dado del futuro. Ahora bien, al revés de los virus o los gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; por eso, de todos los dispositivos informáticos criminales, las bombas lógicas son las que poseen el máximo potencial de daño. Su detonación puede programarse para que cause el máximo de daño y para que tenga lugar mucho tiempo después de que se haya marchado el delincuente. La bomba lógica puede utilizarse también como instrumento de extorsión y se puede pedir un rescate a cambio de dar a conocer el lugar en donde se halla la bomba.

4.1.10. Gusanos.- Se fabrica de forma análoga al virus con miras a infiltrarlo en programas legítimos de procesamiento de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse. En términos médicos podría decirse que un gusano es un tumor benigno, mientras que el **virus.-** es un tumor maligno. Ahora bien, las consecuencias del ataque de un gusano pueden ser tan graves como las del ataque de un virus: por ejemplo, un programa gusano que subsiguientemente se destruirá

puede dar instrucciones a un sistema informático de un banco para que transfiera continuamente dinero a una cuenta ilícita"[13].

4.1.11. Virus informáticos y malware.-

"Son elementos informáticos, que como los microorganismos biológicos, tienden a reproducirse y a extenderse dentro del sistema al que acceden, se contagian de un sistema a otro, exhiben diversos grados de malignidad y son eventualmente, susceptibles de destrucción con el uso de ciertos antivirus, pero algunos son capaces de desarrollar bastante resistencia a estos"[14].

Un virus puede ingresar en un sistema por conducto de una pieza legítima de soporte lógico que ha quedado infectada, así como utilizando el método del Caballo de Troya. Han sido definidos como "pequeños programas que, introducidos subrepticiamente en una computadora, poseen la capacidad de auto-reproducirse sobre cualquier soporte apropiado que tengan acceso al computador afectado, multiplicándose en forma descontrolada hasta el momento en que tiene programado actuar.

El malware es otro tipo de ataque informático, que usando las técnicas de los virus informáticos y de los gusanos y las debilidades de los sistemas desactiva los controles informáticos de la máquina atacada y causa que se propaguen los códigos maliciosos.

[13] ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador
[14] GUIBOURG Ricardo A., Delitos de la información. Madrid España.

4.1.12. Ciberterrorismo.-

"Terrorismo informático es el acto de hacer algo para desestabilizar un país o aplicar presión a un gobierno, utilizando métodos clasificados dentro los tipos de delitos informáticos"[15]

Especialmente los de los de tipo de Sabotaje, sin que esto pueda limitar el uso de otro tipo de delitos informáticos, además lanzar un ataque de terrorismo informático requiere de muchos menos recursos humanos y financiamiento económico que un ataque terrorista común.

4.1.13. Ataques de denegación de Servicio.-

"se basan en utilizar la mayor cantidad posible de recursos del sistema operativo, de manera que nadie más pueda usarlos, perjudicando así seriamente la actuación del sistema, especialmente si debe dar servicio a mucho usuarios"[16]

Como ejemplos típicos de este ataque son el consumo de memoria de la máquina víctima, hasta que se produce un error general en el sistema por falta de memoria, lo que la deja fuera de servicio, la apertura de cientos o miles de ventanas, con el fin de que se pierda el foco del ratón y del teclado, de manera que la máquina ya no responde a pulsaciones de teclas o de los

[15]MANUAL de Informática Jurídica, Editorial Astrea, 1996, Buenos Aires.
[16]MANUAL de Informática Jurídica, Editorial Astrea, 1996, Buenos Aires.

botones del ratón, siendo así totalmente inutilizada, en máquinas que deban funcionar ininterrumpidamente, cualquier interrupción en su servicio por ataques de este tipo puede acarrear consecuencias desastrosas.

4.1.14. El espionaje informático y el robo o hurto de software:

4.1.14.1. Fuga de datos (Data Leakage)(también conocida como la divulgación no autorizada de datos reservados),

"Es una variedad del espionaje industrial que sustrae información confidencial de una empresa. A decir de Luis Camacho Loza, "la facilidad de existente para efectuar una copia de un fichero mecanizado es tal magnitud en rapidez y simplicidad que es una forma de delito prácticamente al alcance de cualquiera"[17].

4.1.15. El robo de servicios:

4.1.15.1. Hurto del tiempo del computador.-

"Consiste en el hurto del tiempo de uso de las computadoras, en el cual una empresa proveedora de este servicio proporciona una clave de acceso al usuario de Internet, para que con esa clave pueda acceder al uso de la supercarretera de la información, pero sucede que el usuario de ese servicio da esa clave a otra persona que no está autorizada para usarlo, causándole un perjuicio patrimonial a la empresa proveedora de servicios"[18].

4.1.15.2. Apropiación de informaciones residuales(SCAVENGING).-

[17]CAMACHO LOSA, Luis, El Delito Informático, Madrid, España, 1987.
[18]MANUAL de Informática Jurídica, Editorial Astrea, 1996, Buenos Aires.

"Es el aprovechamiento de la información abandonada sin ninguna protección como residuo de un trabajo previamente autorizado. Toscavenge, se traduce en recoger basura. Puede efectuarse físicamente cogiendo papel de desecho de papeleras o electrónicamente, tomando la información residual que ha quedado en memoria o soportes magnéticos"[19].

4.1.16. Parasitismo Informático (PIGGYBACKING) y suplantación de personalidad (IMPERSONATION).-

Figuras en que concursan a la vez los delitos de suplantación de personas o nombres y el espionaje, entre otros delitos. En estos casos,

"el delincuente utiliza la suplantación de personas para cometer otro delito informático. Para ello se prevale de artimañas y engaños tendientes a obtener, vía suplantación, el acceso a los sistemas o códigos privados de utilización de ciertos programas generalmente reservados a personas en las que se ha depositado un nivel de confianza importante en razón de su capacidad y posición al interior de una organización o empresa determinada"[20].

4.1.17.1. El acceso no autorizado a servicios informáticos:Las puertas falsas (TRAPDOORS).-

"consiste en la práctica de introducir interrupciones en la lógica de los programas con el objeto de chequear en medio de procesos complejos, si los resultados intermedios son correctos, producir salidas de control con el mismo fin o guardar resultados intermedios en ciertas áreas para comprobarlos más adelante"[21].

[19]MANUAL de Informática Jurídica, Editorial Astrea, 1996, Buenos Aires.
[20]MANUAL de Informática Jurídica, Editorial Astrea, 1996, Buenos Aires.
[21]MANUAL de Informática Jurídica, Editorial Astrea, 1996, Buenos Aires.

4.1.17.2. La llave Maestra (SUPERZAPPING).-

"es un programa informático que abre cualquier archivo del computador por muy protegido que esté, con el fin de alterar, borrar, copiar, insertar o utilizar, en cualquier forma no permitida, datos almacenados en el computador"[22]

Su nombre deriva de un programa utilitario llamado *superzap*, que es un programa de acceso universal, que permite ingresar a un computador por muy protegido que se encuentre, es como una especie de llave que abre cualquier rincón del computador. Mediante esta modalidad es posible alterar los registros de un fichero sin que quede constancia de tal modificación.

4.1.17.3. Pinchado de líneas (WIRETAPPING).-

"consiste en interferir las líneas telefónicas de transmisión de datos para recuperar la información que circula por ellas, por medio de un radio, un módem y una impresora".

Como se señaló anteriormente el método más eficiente para proteger la información que se envía por líneas de comunicaciones es la criptografía que consiste en la aplicación de claves que codifican la información, transformándola en un conjunto de caracteres ininteligibles de letras y números sin sentido aparente, de manera tal que al ser recibida en destino, y

[22]MANUAL de Informática Jurídica, Editorial Astrea, 1996, Buenos Aires.

por aplicación de las mismas claves, la información se recompone hasta quedar exactamente igual a la que se envió en origen.

4.1.17.4. Piratas Informáticos o Hackers.-

"El acceso se efectúa a menudo desde un lugar exterior, situado en la red de telecomunicaciones, recurriendo a uno de los diversos medios que se mencionan a continuación. El delincuente puede aprovechar la falta de rigor de las medidas de seguridad para obtener acceso o puede descubrir deficiencias en las medidas vigentes de seguridad o en los procedimientos del sistema. A menudo, los piratas informáticos se hacen pasar por usuarios legítimos del sistema; esto suele suceder con frecuencia en los sistemas en los que los usuarios pueden emplear contraseñas comunes o contraseñas de mantenimiento que están en el propio sistema"[23].

4.1.18. Reproducción no autorizada de programas informáticos de protección legal.-

Esta puede entrañar una pérdida económica sustancial para los propietarios legítimos. Algunas jurisdicciones han tipificado como delito esta clase de actividad y la han sometido a sanciones penales. El problema ha alcanzado dimensiones transnacionales con el tráfico de esas reproducciones no autorizadas a través de las redes de telecomunicaciones modernas. Al respecto, considero, que la reproducción no autorizada de programas informáticos no es un delito informático, debido a que, en primer lugar el bien jurídico protegido es en este caso el derecho de autor, la propiedad intelectual y en segundo lugar que la protección al software es uno de los

[23]MANUAL de Informática Jurídica, Editorial Astrea, 1996, Buenos Aires.

contenidos específicos del Derecho informático al igual que los delitos informáticos, por tal razón considero que la piratería informática debe ser incluida dentro de la protección penal al software y no estar incluida dentro de las conductas que componen la delincuencia informática.

4.1.19. Delito Informático.-.

"Son los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas redes y datos"[24]

4.1.20. Comercio Electrónico.-

"El comercio electrónico consiste en realizar electrónicamente transacciones comerciales. Está basado en el tratamiento y transmisión electrónica de datos, incluidos texto, imágenes y vídeo. El comercio electrónico comprende actividades muy diversas, como comercio electrónico de bienes y servicios, suministro en línea de contenidos digitales, transferencia electrónica de fondos, compraventa electrónica de acciones, conocimientos de embarque electrónicos, subastas, diseños y proyectos conjuntos, prestación de servicios en línea (on line sourcing), contratación pública, comercialización directa al consumidor y servicios posventa. Por otra parte, abarca a la vez productos (p.ej., bienes de consumo, equipo médico especializado) y servicios (p.ej., servicios de información, financieros y jurídicos), actividades tradicionales (p.ej., asistencia sanitaria, educación) y nuevas actividades (p.ej., centros comerciales virtuales)[25].

4.1.21. Infracción Informática.-

[24] El Convenio de Cyber-delincuencia del Consejo de Europa
[25] WIKIPEDIA. http://es.wikipedia.org/wiki/Internet.07/11/2011

"Infracciones relacionadas con los Ordenadores", "Crímenes por Ordenador", etc., son aquellas "conductas que ponen en peligro o lesionan la integridad, confidencialidad y/o disponibilidad de los datos y sistemas informáticos, y ello sin perjuicio de que, además, puedan suponer una puesta en peligro y lesión de bienes jurídicos distintos"[26]

4.1.22. La firma electrónica

"Es una firma digital que se ha almacenado en un soporte La ***firma electrónica*** *es una firma digital que se ha almacenado en un soporte hardware; mientras que la firma digital se puede almacenar tanto en soportes hardware como software. La firma electrónica reconocida tiene el mismo valor legal que la firma manuscrita. A pesar del uso indistinto que se suele hacer de los términos firma electrónica y firma digital, entre los profesionales del tema se hace una clara diferenciación entre estos.; mientras que la firma digital se puede almacenar tanto en soportes hardware como software. La firma electrónica reconocida tiene el mismo valor legal que la firma manuscrita. A pesar del uso indistinto que se suele hacer de los términos firma electrónica y firma digital, entre los profesionales del tema se hace una clara diferenciación entre estos.*

Las diferentes definiciones que he citado y muchas más son coincidentes en manifestar que la infracción o delito informático es todo acto intencional, provocado por persona o personas, asociado de una manera u otra a los computadores; en los cuales intervienen de forma directa dos sujetos, por una parte el sujeto pasivo que es la víctima que ha o habría podido sufrir un daño o pérdida; y el sujeto activo constituido por el autor que ha o habría podido obtener un beneficio del acto[27]*".*

Es preciso señalar a estas alturas del trabajo un concepto que reúna en si todos los aspectos de nuestro interés es por ello que los autores chilenos

[26]VALLEJO María Cristina, Derecho Financiero y Bursatil, Quito Ecuador

[27]http://es.wikipedia.org/wiki/Firma_electr%C3%B3nica

HUERTA MIRANDA, Marcelo y LÍBANO MANZUR Claudio, en su obra Los Delitos Informáticos, nos señalan lo siguiente:

"*Debido a que el concepto a definir es un concepto inmerso en el derecho, no nos cabe duda que son precisamente los expertos de este mundo-ciencia los llamados irrefutablemente a diseñar la definición de los delitos informáticos. El derecho es una ciencia llamada a regular todos los tópicos de la vida en sociedad y especialmente a salvaguardaría, sobre principios de justicia, de los atentados a la normal y pacífica convivencia. Desde esta perspectiva, el derecho debe entregar la definición del Derecho Informático y por ende de sus delitos, en relación de continente a contenido. Se podrá decir que el jurista no está capacitado para indagar en los fenómenos de la informática y que por lo tanto la definición debe provenir de aquellos que han abrazado ciencias relacionadas con ella. Sin ánimo de polemizar, decimos que el Derecho como expresión normativa de la Justicia regula todos los aspectos de la convivencia social, incluida la actividad informática que se aplica en toda actividad humana, con tanta trascendencia social y económica. Para tan alta empresa, el derecho, muchas veces se auxilia en los conocimientos propios de otras ciencias, a los cuales les aplica su sello distintivo constructor de normas y principios jurídicos. Pensar lo contrario, implicaría imposibilitar al mundo del derecho de normar sobre la medicina forense, las ingenierías, las ciencias que abarcan la expresión pública, etc. Aún más grave, se pondría al juez, que es un abogado, en la imposibilidad de administrar justicia en materias ajenas al derecho*."[28]

Lo señalado por los juristas chilenos, nos permiten ampliar claramente el panorama, en el sentido que estamos ante un asunto a más de técnico es jurídico, siendo fundamental que los jurisconsultos analicen este aspecto desde el campo legal, para que propongan las alternativas válidas para solucionar este problema que cada vez aqueja a mayores sectores de la sociedad.

[28]HUERTA MIRANDA, Marcelo y LÍBANO MANZUR Claudio**,** Los DelitosInformáticos, Editorial Jurídica Cono Sur.

4.2. MARCO DOCTRINARIO.

4.2.1. El Delito Informático y su realidad procesal en el Ecuador.

¨Desde que en 1999 en el Ecuador se puso en el tapete de la discusión el proyecto de Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, desde ese tiempo se puso de moda el tema, se realizaron cursos, seminarios, encuentros. También se conformó comisiones para la discusión de la Ley y para que formulen observaciones a la misma por parte de los organismos directamente interesados en el tema como el CONATEL, la Superintendencia de Bancos, las Cámaras de Comercio y otros, que ven el Comercio Telemático una buena oportunidad de hacer negocios y de paso hacer que nuestro país entre en el boom de la llamada Nueva Economía¨[29]

En nuestro país en ese año nos encontrábamos con que el ordenamiento jurídico en materia penal, no había avanzado en estos últimos tiempos a diferencia de otras legislaciones, por tanto era necesario para enfrentar a la llamada criminalidad informática que los tipos penales tradicionales sean reformados, sean actualizados para así consolidar la seguridad jurídica en el Ecuador, ya que 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. Esta clase de conductas reprochables resultan en la mayoría de los casos impunes, debido a la falta de conocimiento y preparación de los organismos de administración de justicia y los cuerpos policiales.

[29]ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador

En este orden de ideas, y al verse la posibilidad, que por medio del uso indebido de los sistemas informáticos o telemáticos se dé paso a la manipulación de sistemas de hospitales, aeropuertos, parlamentos, sistemas de seguridad, sistemas de administración de justicia, etc. Nos permiten imaginar incontables posibilidades de comisión de conductas delictivas de distintas características, por eso es necesario que el Ministerio Público en cumplimiento de su deber constitucional y legal instruya y facilite las herramientas necesarias a los Ministros Fiscales, Agentes Fiscales y personal de Apoyo a fin de combatir esta clase de comportamientos delictivos que afectan directamente a la sociedad ecuatoriana en su conjunto.

¨Cuando la ley se presentó en un principio, tenía una serie de falencias, que con el tiempo se fueron puliendo, una de ellas era la parte penal de dicha ley, ya que las infracciones a la misma es decir los llamados Delitos Informáticos, como se los conoce, se sancionarían de conformidad a lo dispuesto en nuestro Código Penal, situación como comprenderán era un tanto forzada, esto si tomamos en cuenta los 65 años de dicho Código, en resumen los tipos penales ahí existentes, no tomaban en cuenta los novísimos adelantos de la informática y la telemática por tanto les hacía inútiles por decirlo menos, para dar seguridad al Comercio Telemático ante el posible asedio de la criminalidad informática.

Por fin en abril del 2002 y luego de largas discusiones los honorables diputados por fin aprobaron el texto definitivo de la Ley de Comercio Electrónico, Mensajes de Datos y Firmas Electrónicas, y en consecuencia las reformas al Código Penal que daban la luz a los llamados Delitos Informáticos.¨[30]

La Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos (LCElec.) fue publicada en el Registro Oficial N° 557 del 17 de Abril del 2002

[30]ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador

en el que se dispone que los mensajes de datos tendrán, igual valor jurídico que los documentos escritos.

La Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos está conformada por cinco títulos conteniendo cada uno varios capítulos y artículos

Título Preliminar.

De las Firmas electrónicas, certificados de firmas electrónicas, entidades de certificación de información, organismos de promoción de los servicios electrónicos, y de regulación y control de las entidades de certificación acreditadas.

De los servicios electrónicos, la contratación electrónica y telemática, los derechos de los usuarios, e instrumentos públicos. De la prueba y notificaciones electrónicas.

4.2.1.1. **De las infracciones informáticas**.

La Ley contiene los principios jurídicos que regirán las transmisiones de los mensajes de datos. Se le concede pleno valor y eficacia jurídica a los mensajes de datos, tanto a su información como a su contenido general; la interpretación de la Ley y el ejercicio de la Propiedad Intelectual se rigen por

la legislación ecuatoriana y por los tratados internacionales incorporados al cuerpo legal ecuatoriano. Se protege la confidencialidad de los mensajes de datos en sus diversas formas, señalando lo que se entenderá por tal concepto y su violación. Se equipara el documento escrito con el documento electrónico para el caso en que se requiera la presentación de un documento escrito, procediendo de igual manera con el documento original y la información contenida en él, siempre y cuando exista garantía de su conservación inalterable.

¨Esto en concordancia con el Art. 33 del Código de Procedimiento Penal que señala que "el ejercicio de la acción pública corresponde exclusivamente al fiscal". De lo dicho podemos concluir que el dueño de la acción penal y de la investigación tanto pre procesal como procesal de hechos que sean considerados como delitos dentro del nuevo Sistema Procesal Penal Acusatorio es el Fiscal. Es por tanto el Fiscal quien deberá llevar como quien dice la voz cantante dentro de la investigación de esta clase de infracciones de tipo informático para lo cual contara como señala el Art. 208 del Código de Procedimiento Penal con su órgano auxiliar la Policía Judicial quien realizará la investigación de los delitos de acción pública y de instancia particular bajo la dirección y control Ministerio Público, en tal virtud cualquier resultado de dichas investigaciones se incorporaran en su tiempo ya sea a la Instrucción Fiscal o a la Indagación Previa, esto como parte de los elementos de convicción que ayudaran posteriormente al representante del Ministerio Público a emitir su dictamen correspondiente.¨[31]

Al determinar al fiscal el ejercicio de la acción pública dentro del procedimiento penal para que estas infracciones informáticas sean consideradas como delitos se debe confiar que actué con severidad para que estas infracciones no pasen desapercibidas ante la sociedad.

[31]ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador

¨Por tanto es esencial que se formen unidades Investigativas tanto policiales como del Ministerio Público especializadas en abordar cuestiones de la delincuencia informática trasnacional y también a nivel nacional. Estas unidades pueden servir también de base tanto para una cooperación internacional formal o una cooperación informal basada en redes transnacionales de confianza entre los agentes de aplicación de la ley. Lo cual es posible aplicando la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos¨[32].

¨De otro lado en los últimos tiempos la masificación de virus informáticos globales, la difusión de la pornografía infantil e incluso actividades terroristas son algunos ejemplos de los nuevos delitos informáticos y sin fronteras que presentan una realidad difícil de controlar. Con el avance de la tecnología digital en los últimos años, ha surgido una nueva generación de delincuentes que expone a los gobiernos, las empresas y los individuos a estos peligros.¨ [33]

Empresas de toda índole y a nivel Mundial han sido perjudicadas por esta clase de delitos que a menudo son personas que están inmersas en el campo de la informática y con elevadas posibilidades de que no lleguen a descubrirles. Por lo tanto, se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos. Al unir una red a la Internet, se tiene acceso a las redes de otras

El sabotaje informático, es llevado a cabo, en la mayoría de los casos por empleados descontentos y puede producirse, tanto a la parte física del ordenador (hardware) como a la parte lógica del mismo (software). Los daños al software se pueden causar a través de elementos electromagnéticos, cuyas técnicas son las siguientes: la introducción de

[32] ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador
[33] ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador

virus, gusanos o una bomba lógica que destruye, altere o inutilice los programas, datos o documentos electrónicos almacenados en el sistema informático.

Qué son los virus?.- Es una serie de instrucciones de programación que pueden adherirse a los programas legítimos y propagarse a otros programas informáticos. Un virus puede ingresar al sistema por conducto de un soporte lógico (fllopy, CDROM, etc) que ha quedado infectada, así como utilizando el método del Caballo de Troya.

Qué son los gusanos? Son aquellos que se fabrican de forma lógica al virus y su intención es infiltrarse en programa de procesamientos de datos o para modificar o destruir los datos, pero es diferente del virus porque no puede regenerarse, por lo tanto no es tan grave como el virus.

Qué es la bomba lógica o cronológica? Es aquella que exige conocimientos especializados, ya que requiere la programación de la destrucción o modificación de datos. Es importante destacar, que a diferencia de los virus o gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; es por esta razón, que de todos los dispositivos informáticos criminales, la bomba lógica es la que más daño hace dentro del sistema informático. Es difícil saber cuál es el sujeto, por cuanto se puede programar la detonación para que tenga lugar mucho tiempo después de que se haya marchado el criminal informático.

Es muy importante diferenciar entre el Hacking y Cracking, el primero, utiliza técnicas de penetración no programadas para acceder a un sistema informático, buscando únicamente el ingreso a tales sistemas sin dirigir sus actos a la afectación de la integridad o disponibilidad de la información, pero sí a la confidencialidad y exclusividad de la misma y también en algunos casos a vulnerar la intimidad del titular de aquella; mientras que el segundo, altera, suprime o daña la información, por cuanto la intención del agente es obstaculizar, dejar inoperante o menoscabar el funcionamiento de un sistema o dato informático.

Organizaciones también unidas. Es así, que podemos acceder a la oficina de enfrente de nuestra empresa, podemos recibir información de un servidor en Japón, conectarnos a una supercomputadora en Washington o revisar la literatura disponible desde Francia. Del universo de varias decenas de millones de computadoras interconectadas, no es difícil pensar que puede haber más de alguien con perversas intenciones respecto a nuestra organización, es por esta razón, que debemos tener nuestra red protegida adecuadamente, para no ser tal vulnerable a los ataques informáticos de personas inescrupulosas

¨Es por estas razones que el Ministerio Público tiene la obligación Jurídica en cumplimiento de su mandato constitucional de poseer un cuerpo especializado para combatir esta clase de criminalidad a fin de "precautelar los derechos de las víctimas y llevar a los responsables a juicio, terminando así con la cifra negra de esta clase de infracciones, ya que en la actualidad esta clase de conductas ilícitas no son tratadas en debida forma por los órganos llamados a su persecución e investigación, así por ejemplo un tipo

de delito actualmente en boga en nuestro país es el llamado CARDING (utilización de tarjetas magnéticas, ya sean hurtadas o clonadas para defraudar mediante la técnica de manipulación de datos de salida) y, el cual que es una modalidad de Fraude Informático, mismo que es considerado por la Policía Judicial como una clase de estafa, lo que desde el punto de vista de la clasificación típica del delito es incorrecta ya que no es una estafa, tomando en cuenta los elementos típicos de este tipo de delitos, lo que sí es una clase de defraudación, pero la solución doctrinaria y típica a dicha modalidad delictual es equipararla al robo calificado, en razón que la tarjeta magnética es considerada como una llave."[34]

La clonación de tarjetas es uno de los principales fraudes que sufren los usuarios. La mayor de las veces ocurre dentro de un cajero automático, para saber cómo los delincuentes pueden clonar una tarjeta de crédito no te pierdas esta importante información.

En primer lugar, hay que conocer cómo actúa el Skimmer (Dispositivo electrónico que lee tarjetas de crédito).

Este nueva herramienta se introduce en los cajeros, en el mismo lugar donde los usuarios colocan la tarjeta, lo que realiza este dispositivo es leer la banda magnética del plástico, y a través de una computadora pasa los datos a una tarjeta vacía, de esta manera "clona" una tarjeta.

Esto permite traspasar no sólo los datos, como el NIP, sino también los datos de la cuenta bancaria.

[34]ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador

Hay casos en el que un tarjeta habiente desea realizar una extracción de efectivo desde un cajero, y cuando tiene que retirar el dinero no sale, entonces posiblemente acuda a otro cajero automático, y al querer realizar la operación nota que su cuenta ha sido vaciada.

4.2.2. GENERALIDADES DEL COMERCIO ELECTRONICO.

La Ley de comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, en su Título Primero **DE LOS MENSAJES DE DATOS**, señala entre los principios Generales entre otros los siguientes:

Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta Ley y su reglamento.

Se reconoce validez jurídica a la información no contenida directamente en un mensaje de datos, siempre que figure en el mismo, en forma de remisión o de anexo accesible mediante un enlace electrónico directo y su contenido sea conocido y aceptado expresamente por las partes.

Los mensajes de datos estarán sometidos a las leyes, reglamentos y acuerdos internacionales relativos a la propiedad intelectual.

Para poder comprender de mejor manera vamos analizar algunos términos importantes:

4.2.2.1. COMERCIO ELECTRÓNICO.

El **comercio electrónico**, también conocido como *e-commerce* (*electroniccommerce* en inglés), consiste en la compra y venta de productos o de servicios a través de medios electrónicos, tales como Internet y otras redes informáticas. Originalmente el término se aplicaba a la realización de transacciones mediante medios electrónicos tales como el Intercambio electrónico de datos, sin embargo con el advenimiento de la Internet y la World Wide Web a mediados de los años 90 comenzó a referirse principalmente a la venta de bienes y servicios a través de Internet, usando como forma de pago medios electrónicos, tales como las tarjetas de crédito.

4.2.2.2. FIRMAS ELECTRONICAS.

Es la equivalencia digital de la firma manuscrita, tiene la misma validez legal y se encuentra amparada por la **Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.**

La firma digital permite la transacción segura de documentos y operaciones en aplicaciones computacionales garantizando los siguientes aspectos:

- **Identidad**, reconoce unívocamente a un emisor como autor del mensaje.

- **Integridad**, el documento no puede ser alterado de forma alguna durante la transmisión.

- **No repudio**, el emisor no puede negar en ningún caso que un documento no fue firmado.

- **Confidencialidad**, solo las partes puedan leer el documento (si fuera el caso).

4.2.2.3. USO DE LA FIRMA ELECTRÓNICA.

Con la firma electrónica pueden realizarse diferentes tipos de transacciones a través de la Internet sin necesidad de desplazarse, ni hacer filas de forma que los trámites públicos se agilitan aumentando la transparencia, lo que se traduce en ahorros significativos de tiempo y dinero. Las aplicaciones de la firma digital son diversas. Se cita algunas de ejemplo a continuación:

• Compras públicas
• Trámites ciudadanos (Gobierno electrónico)
• Gestión documental

• Operaciones bancarias

• Dinero (pago) electrónico

• Balances electrónicos

• Trámites judiciales y notariales

• Comercio electrónico

• Facturación electrónica

Desde el punto de vista técnico, la firma es un conjunto de datos digitales que se añaden a un archivo digital y que se obtienen del cifrado del mismo mediante programas computacionales.

4.2.3. TIPOS DE DELITOS INFORMÁTICOS.

Existen muchos tipos de delitos informáticos, la diversidad de comportamientos constitutivos de esta clase de ilícitos es escandaloso, no existen límites para estas personas, utilizan su imaginación, y capacidad técnica todo ello conjugado con las deficiencias de control existentes en las instalaciones informáticas, poder caracterizar o establecer los diferentes tipos resulta complicado pero con el fin de presentar un aporte didáctico me permito señalar varios de ellos.

4.2.3.1. LOS DATOS FALSOS O ENGAÑOSOS.

¨Este tipo de fraude informático conocido también como manipulación de datos de entrada, representa el delito informático más común ya que es fácil

de cometer y difícil de descubrir. Este delito no requiere de conocimientos técnicos de informática y puede realizarlo cualquier persona que tenga acceso a las funciones normales de procesamiento de datos en la fase de adquisición de los mismos.¨[35]

Se conoce a este tipo de delito como la introducción de datos falsos, esto realizando la maniobra e introducción de datos en equipos de computación cuya finalidad es producir movimientos falsos en transacciones de instituciones o empresas.

4.2.3.2. FALSIFICACIONES INFORMÁTICAS:

¨Cuando empezó a disponerse de fotocopiadoras computarizadas en color basándose en rayos láser surgió una nueva generación de falsificaciones o alteraciones fraudulentas. Estas fotocopiadoras pueden hacer reproducciones de alta resolución, pueden modificar documentos e incluso pueden crear documentos falsos sin tener que recurrir a un original, y los documentos que producen son de tal calidad que sólo un experto puede diferenciarlos de los documentos auténticos.¨[36]

Para una mejor compresión podemos analizar este tipo de falsificaciones desde dos aspectos fundamentales e importantes, como lo son, desde el punto de vista de objeto, que es cuando las personas inescrupulosas producen la alteración de datos en los documentos que constan almacenados de forma digital o magnética en un computador, sistema informáticos de almacenamiento; y, desde el punto de vista de instrumento,

[35] MAGLIONA MARKOVICTH Claudio Paúl, LÓPEZ MEDEL Macarena, Delincuencia y Fraude Informático, Editorial Jurídica de Chile. 1999
[36] MAGLIONA MARKOVICTH Claudio Paúl, LÓPEZ MEDEL Macarena, Delincuencia y Fraude Informático, Editorial Jurídica de Chile. 1999

actos en los que se emplean equipos informáticos para la materialización de falsificaciones de documentos en general, es decir pueden ser documentos de uso público, financiero o comercial.

4.2.3.3. MANIPULACIÓN DE LOS DATOS DE SALIDA.

¨Se efectúa fijando un objetivo al funcionamiento del sistema informático, en la actualidad se usan ampliamente equipo y programas de computadora especializados para codificar información electrónica falsificada en las bandas magnéticas de las tarjetas bancarias y de las tarjetas de crédito.¨[37]

La mejor manera de comprender esta forma de delito es trasladándonos imaginariamente a la realidad, y es que con gran frecuencia se puede observar a través de los medios de comunicación los fraudes de que se cometen en los cajeros automáticos de las diferentes instituciones financieras, mediante la falsificación de instrucciones para la computadora en la fase de adquisición de dato, así como empleando diferentes artefactos lectores de bandas magnéticas, utilizando cámaras de video en las cuales se registran todas las pulsaciones que realizan los usuarios de las diferentes tarjetas de débito o tarjetas de crédito.

[37] MAGLIONA MARKOVICTH Claudio Paúl, LÓPEZ MEDEL Macarena, Delincuencia y Fraude Informático, Editorial Jurídica de Chile. 1999

4.3. MARCO JURÍDICO.

Nuestra legislación en algunos tópicos aborda esta problemática motivo por el cual citare las diferentes disposiciones legales relacionadas directamente al tema materia de la presente investigación.

El Ecuador bajo el contexto de que la información es un bien jurídico a proteger, se mantienen leyes y decretos que establecen apartados y especificaciones acorde con la importancia de las tecnologías, tales como:

1) Constitución de la República del Ecuador.

2) Ley Orgánica de Transparencia y Acceso a la Información Pública.

3) Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

4) Ley de Propiedad Intelectual.

5) Ley Especial de Telecomunicaciones.

6) Ley de Control Constitucional (Reglamento Habeas Data).

7) Código de procedimiento Penal.

8) Código Penal.

4.3.1 CONSTITUCION DE LA REPUBLICA DEL ECUADOR.

En la Constitución de la República del Ecuador vigente en el Título II de los Derechos, en la Sección Tercera, de la Comunicación e Información manifiesta que:

Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.
2. El acceso universal a las tecnologías de información y comunicación.
3. La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radio eléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas.
4. El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad.
5. Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación[38].

[38] Constitución de la República del Ecuador Art. 16.

El Estado fomentará la pluralidad y la diversidad en la comunicación, y al efecto:

1. Garantizará la asignación, a través de métodos transparentes y en igualdad de condiciones, de las frecuencias del espectro radio eléctrico, para la gestión de estaciones de radio y televisiones públicas, privadas y comunitarias, así como el acceso a bandas libres para la explotación de redes inalámbricas, y precautelará que en su utilización prevalezca el interés colectivo.

2. Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación, en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada.

3. No permitirá el oligopolio o monopolio, directo ni indirecto, de la propiedad de los medios de comunicación y del uso de las frecuencias[39].

Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimiento y procesos de interés general, y con responsabilidad ulterior.

2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente

[39] Constitución de la República del Ecuador Art. 17.

establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información[40].

La ley regulará la prevalencia de contenidos con fines informativos, educativos y culturales en la programación de los medios de comunicación, y fomentará la creación de espacios para la difusión de la producción nacional independiente.

Se prohíbe la emisión de publicidad que induzca a la violencia, la discriminación, el racismo, la toxicomanía, el sexismo, la intolerancia religiosa o política y toda aquella que atente contra los derechos[41].

El Estado garantizará la cláusula de conciencia a toda persona, y el secreto profesional y la reserva de la fuente a quienes informen, emitan sus opiniones a través de los medios u otras formas de comunicación, o laboren en cualquier actividad de comunicación[42].

La acción de acceso a la información pública tendrá por objeto garantizar el acceso a ella cuando ha sido denegada expresa o tácitamente, o cuando la que se ha proporcionado no sea completa o fidedigna. Podrá ser interpuesta incluso si la negativa se sustenta en el carácter secreto, reservado, confidencial o cualquiera otra clasificación de la información. El carácter

[40] Constitución de la República del Ecuador Art. 18.
[41] Constitución de la República del Ecuador Art. 19.
[42] Constitución de la República del Ecuador Art. 20.

reservado de la información deberá ser declarado con anterioridad a la petición, por autoridad competente y de acuerdo con la ley[43].

Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Así mismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos.

Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley.

La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta

[43] Constitución de la República del Ecuador Art. 91.

podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados[44].

4.3.2 LEY ORGÁNICA DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

La Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTaip), publicada en el Registro Oficial Suplemento # 337 del 18 de mayo del 2004

La ley establece que todas las instituciones del sector público pongan a disposición de la ciudadanía, el libre acceso a la información institucional (estructura orgánica, bases legales, regulaciones, metas, objetivos, presupuestos, resultados de auditorías, etc.), a través de sus sitios web[45].

Bajo este mismo contexto las disposiciones contenidas en la Constitución de la República del Ecuador vigente, en su Título III, Garantías Constitucionales Capítulo Tercero de las Garantías Jurisdiccionales de sus Secciones Cuarta y Quinta de los Art. 91 y 92 sobre la acción de acceso a la información Pública y Acción de Habeas Data[46].

[44] Constitución de la República del Ecuador Art. 92.
[45] Ley Orgánica de Transparencia y Acceso a la Información Pública.
[46] Constitución de la República del Ecuador Arts.91 y 92 .

4.3.3. LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS.

La Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos (LCElec.) fue publicada en el Registro Oficial N° 557 del 17 de Abril del 2002 en el que se dispone que los mensajes de datos tendrán, igual valor jurídico que los documentos escritos.

La Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos está conformada por cinco títulos conteniendo cada uno varios capítulos y artículos.

Título Preliminar.

De las Firmas electrónicas, certificados de firmas electrónicas, entidades de certificación de información, organismos de promoción de los servicios electrónicos, y de regulación y control de las entidades de certificación acreditadas.

De los servicios electrónicos, la contratación electrónica y telemática, los derechos de los usuarios, e instrumentos públicos.

De la prueba y notificaciones electrónicas.

De las infracciones informáticas[47].

La Ley contiene los principios jurídicos que regirán las transmisiones de los mensajes de datos. Se le concede pleno valor y eficacia jurídica a los mensajes de datos, tanto a su información como a su contenido general; la interpretación de la Ley y el ejercicio de la Propiedad Intelectual se rigen por la legislación ecuatoriana y por los tratados internacionales incorporados al cuerpo legal ecuatoriano. Se protege la confidencialidad de los mensajes de datos en sus diversas formas, señalando lo que se entenderá por tal concepto y su violación. Se equipara el documento escrito con el documento electrónico para el caso en que se requiera la presentación de un documento escrito, procediendo de igual manera con el documento original y la información contenida en él, siempre y cuando exista garantía de su conservación inalterable.

Como punto esencial, se establece que la firma electrónica tendrá validez cuando conste como un requisito de legalidad documental. Además se protege las bases de datos creadas u obtenidas por transmisión electrónica de un mensaje de datos, concediendo al titular de dichos datos el poder para autorizar la disposición de su información, sea que dichos datos fueron obtenidos como usuario de un servicio o sea que fueron obtenidos en el intercambio de mensajes de datos. Se ratifica la defensa legal mediante el Derecho Constitucional de Habeas Data.

[47] Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Se busca que especialmente en los negocios relacionados con el comercio electrónico las notificaciones sean por medio de correo electrónico, estableciéndose obligatoriedad de notificar por éste medio y por el tradicional para el caso de resoluciones sometidas a Tribunales de Arbitraje. El documento electrónico será considerado como medio de prueba con todos sus efectos legales. Para que existan presunciones legales sobre la veracidad de un documento, éste deberá cumplir los principios de integridad e identidad, para justificar la voluntad contractual de obligarse por dicho documento. Aquella parte que niegue la validez de un documento electrónico deberá probar que este no cumple con los requisitos técnicos mencionados anteriormente. Se establecen varios requisitos para la correcta aplicación de la prueba en estos casos, entre ellos señalamos:

La presentación de los soportes necesarios en papel del documento electrónico y los mecanismos para la lectura y verificación de la firma.

La presentación del certificado validado por un proveedor de servicios de certificación.

Los demás mensajes de datos deberán guardar especial atención con la integridad de su contenido. Las pruebas serán juzgadas y valoradas de acuerdo con “la seguridad y fiabilidad con la cual se la verificó, envió, archivó y recibió”. Para una mejor apreciación de la prueba el juzgador contará con el asesoramiento de un perito en la materia, es decir un perito informático.

El organismo facultado para autorizar a las entidades de certificación de información es el Consejo Nacional de Telecomunicaciones, según lo dispuesto en la Ley de Comercio Electrónico, Firmas Digitales y Mensaje de Datos y el Reglamento expedido por el Presidente de la República, mediante Decretos Ejecutivos 3496 (31 de julio del 2002) y 1356 (29 de Septiembre del 2008) en los que se establecen el modelo de Resolución para la Acreditación como Entidad de Certificación, Información y Servicios Relacionados, tal como lo establece el Art. 29 del Capítulo II de la ley.

Las funciones y responsabilidades otorgadas por el Consejo Nacional de Telecomunicaciones, a las entidades de certificación de información y servicios relacionados, es que dichas entidades se encargan de la generación, gestión, administración, custodia y protección de las claves y los certificados de firma electrónica, así como la validación de la identidad e información de los usuarios o solicitantes de firmas electrónicas, mediante el uso de infraestructura y recurso humano capacitado para operar dicha infraestructura con absoluta pericia y confidencialidad. Uno de los organismos que obtuvo la autorización del Consejo Nacional de Telecomunicaciones como Entidad de Certificación es el Banco Central del Ecuador para emitir certificados a personas naturales, jurídicas y funcionarios públicos.

4.3.4. LEY DE PROPIEDAD INTELECTUAL

La Ley de Propiedad Intelectual (LPInt.), publicada en el Registro Oficial N° 320 del 19 de Mayo de 1998, nace con el objetivo de brindar por parte del Estado una adecuada protección de los derechos intelectuales y asumir la defensa de los mismos, como un elemento imprescindible para el desarrollo tecnológico y económico del país.

El organismo nacional responsable por la difusión, y aplicación de las leyes de la Propiedad Intelectual en el Ecuador es el INSTITUTO ECUATORIANO DE PROPIEDAD INTELECTUAL (IEPI), el mismo que cuenta con oficinas en Quito, Guayaquil y Cuenca. Es una persona jurídica de derecho público, con patrimonio propio, autonomía administrativa, económica, financiera, y operativa, con sede en la ciudad de Quito[48].

Dar a conocer la importancia que tiene la Propiedad Intelectual en el Ecuador y su debida aplicación en los sectores económico, industrial, intelectual y de investigación, debe ser tarea no sólo del profesional del derecho, sino de los industriales y empresarios, de las instituciones públicas y privadas, de los centros superiores de estudios e inclusive del propio estado ecuatoriano.

Conocer la propiedad intelectual es también conocer, que uno de los principales problemas que enfrenta esta rama del derecho moderno, es la piratería y falsificación de las obras del intelecto humano, las cuales traen

[48] Ley de Propiedad Intelectual.

graves consecuencias económicas y sociales; a más de los perjuicios de los titulares de derechos de propiedad intelectual, pues esta pérdida no solo afecta a los fabricantes de los productos falsificados, sino a la reducción de ingresos tributarios e inclusive la pérdida de empleos, debido a los efectos negativos resultantes de la mano de obra clandestina, de las labores creativas y de investigación, perjudicando la vitalidad cultural y económica de un país.

Es importante resaltar que la ley incluye en su codificación la protección de bases de datos que se encuentren en forma impresa u otra forma, así como también los programas de ordenador (software) los cuales son considerados como obras literarias.

El estudio de piratería mundial de software, que corresponde al año 2007, realizado por la International Data Corporation (IDC), publicado por la Business Software Alliance, establece que Ecuador mantiene una tasa de piratería de un 66%, que constituyen pérdidas por aproximadamente 33 millones de dólares y representan un incremento del 10% con respecto a la última medición (30 millones de dólares). Las iniciativas dadas para la protección y respeto de las especificaciones de la Ley de Propiedad Intelectual, así como los Derechos de Autor se han desarrollado por campañas de la Business Software Alliance (BSA) tales como “Marca el Límite”, “Anímate 2007”, “Buenos Negocios”, “Evite riesgos, use software legal” como acciones puntuales que impulsan el uso de software legal.

Otro proyecto impulsadopor la BSA es la habilitación del portal “Reporte confidencial sobre piratería de software”, que permite denunciar de manera confidencial la piratería del software en América Latina.

4.3.5. LEY ESPECIAL DE TELECOMUNICACIONES

La Ley Especial de Telecomunicaciones fue publicada en el Registro Oficial N° 996 del 10 de Agosto de 1992, en el que se declara que es indispensable proveer a los servicios de telecomunicaciones de un marco legal acorde con la importancia, complejidad, magnitud tecnología y especialidad de dichos servicios, así como también asegurar una adecuada regulación y expansión de los sistemas radioeléctricos, y servicios de telecomunicaciones a la comunidad que mejore de forma permanente la prestación de los servicios existentes[49].

La Ley Especial de Telecomunicaciones tiene por objeto normar en el territorio nacional la instalación, operación, utilización y desarrollo de toda transmisión, emisión o recepción de signos, señales, imágenes, sonidos e información de cualquier naturaleza por hilo radioelectricidad, medios ópticos y otros sistemas electromagnéticos.

4.3.6. LEY ORGÁNICA DE CONTROL CONSTITUCIONAL

[49] Ley Especial de Telecomunicaciones.

La Ley Orgánica de Control Constitucional (LOCConst.), fue publicada en el Registro Oficial N° 99 del 2 de Julio de 1997 y fue calificada con Jerarquía y carácter de Ley Orgánica, por resolución Legislativa, publicado en Registro Oficial 280 del 8 de Marzo del 2001.

La Ley Orgánica de Control Constitucional, en su Capítulo II del Habeas Data establece que "las personas naturales o jurídicas, nacionales o extranjeras, que desean tener acceso a documentos, bancos de datos e informes que sobre si misma o sus bienes están en poder de entidades públicas, de personas naturales o jurídicas privadas, así como conocer el uso y finalidad que se les haya dado o se les este por dar, podrán imponer el recurso de Habeas Data para requerir las respuestas y exigir el cumplimiento de las medidas tutelares prescritas en esta ley, por parte de las personas que posean tales datos o informaciones[50].

En la Constitución Política del Ecuador vigente hasta el (2008), en su capítulo tercero de las Garantías Jurisdiccionales de su sección quinta Art. 92 sobre la acción de Habeas Data, también se establece recurso jurídico de Habeas Data.

4.3.7. CÓDIGO DE PROCEDIMIENTO PENAL.

[50] Ley Orgánica de Control Constitucional.

De acuerdo a la especificación contemplada en la Ley de Comercio Electrónico, Firmas Digitales y Mensajes de Datos, en su título quinto de las infracciones informáticas, los delitos informáticos que se tipifican, mediante reformas al Código de Procedimiento Penal, se muestran a continuación en la siguiente tabla:

INFRACCIONES INFORMATICAS	REPRESION	MULTAS
Delitos contra la información protegida (CPP Art. 202)	6 meses a 1 año	$500 a $1000
1. Violentando claves o sistemas accede u obtiene información	1 a 3 años	$1.000 - $1500
2. Seguridad nacional o secretos comerciales o industriales	3 a 6 años	$2.000 - $10.000
3. Divulgación o utilización fraudulenta	6 a 9 años	$2.000 - $10.000
4. Divulgación o utilización fraudulenta por custodios	2 meses a 2 años	$1.000 - $2.000
Destrucción maliciosa de documentos (CCP Art. 262)	3 a 6 años	---
Falsificación electrónica (CPP Art. 353)	3 a 6 años	---
Daños informáticos (CPP Art. 415)		
1. Daño dolosamente	6 meses a 3 años	$60 - $150
2. Servicio público o vinculado con la defensa nacional	3 a 5 años	$200 - $600
3. No delito mayor	8 meses a 4 años	$200 - $600
Apropiación ilícita (CPP Art. 553)		
1. Uso fraudulento	6 meses a 5 años	$500 - $1000
2. Uso de medios (claves, tarjetas magnéticas, otros instrumentos	1 a 5 años	$1.000 - $2.000
Estafa (CPP Art. 563)	5 años	$500 - 1.000

Infracciones informáticas.

Hemos visto la definición de los delitos informáticos, su principal insumo que es la evidencia digital y las técnicas o mecanismos con los procedimientos existentes para su investigación, vale destacar, entonces que los profesionales dedicados a la persecución de actos ilícitos en los que se utilizan medios tecnológicos, se mantengan a la vanguardia de conocer los avances que se den de ésta índole, y de esta manera mantenerse preparados y reaccionar de manera adecuada ante los actos cometidos por la delincuencia informática.

Ecuador ha dado sus primero pasos con respecto a las leyes existentes, en las que se contemplan especificaciones de la información y la informática, lo que se considera un avance importante ante el desarrollo tecnológico que se ha tenido en los últimos años en el país, pero es evidente que aún falta mucho por legislar, para asegurar que no queden en la impunidad los actos que se comentan relacionados con las tecnologías.

4.3.8. CÓDIGO PENAL.

En el Libro Segundo del Código Penal TITULO II, DE LOS DELITOS CONTRA LAS GARANTIAS CONSTITUCIONALES Y LA IGUALDAD RACIAL, en el CAPITULO V, De los delitos contra la inviolabilidad del secreto, en su Art. 202 A, se determina:

"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, será sancionada 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 realiza 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"[51].

"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."[52]

En el Título III del libro anteriormente señalado se hace referencia a LOS DELITOS CONTRA LA ADMINISTRACION PUBLICA, Capítulo V, De la

[51] Código Penal, Ecuatoriano, Art. 202 A.
[52] Código Penal Ecuatoriano Art. 202 B.

Violación de los deberes de Funcionarios Públicos, de la Usurpación de Atribuciones y de los Abusos de Autoridad, y en su Art. 262 señala:

"Serán reprimidos con tres 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 sin razón de su cargo."[53]

Más adelante en el Titulo IV, DE LOS DELITOS CONTRA LA FE PUBLICA. En su capítulo III, De las Falsificaciones de Documentos en General en su Art. 353 A).

"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.
4.- El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo."[54]

[53] Código Penal Ecuatoriano Art. 262.
[54] Código Penal Ecuatoriano Art. 353 A

En el Titulo V. DE LOS DELITOS CONTRA LA SEGURIDAD PUBLICA. Capítulo VII: del incendio y otras Destrucciones, de los deterioros y daños, en el Art. 415 A) y 415 B) determinan:

"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 seiscientos 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 vinculada con la defensa nacional."[55]

Art. 415 B. 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 seiscientos dólares de los Estados Unidos de Norteamérica."[56]

4.4. LEGISLACIÓN COMPARADA.

4.4.1. Alemania.

En primer lugar me permitiré enunciar algunas disposiciones legales, determinadas en la Legislación Alemana, que ante los brotes de la delincuencia relacionada con la informática, implanto a partir del año 1986,

[55] Código Penal Ecuatoriano Art. 415 A
[56] Código Penal Ecuatoriano Art. 415B

exactamente desde el primero de agosto, dictándose la Según la Ley contra la Criminalidad Económica en la que se contemplan los siguientes delitos:

- *¨Espionaje de datos (art. 202)*
- *Estafa informática (art. 263)*
- *Falsificación de datos probatorios (art. 269) junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos(arts. 270, 271, 273)*
- *Alteración de datos (art. 303 a) es ilícito cancelar, inutilizar o alterar datos inclusive la tentativa es punible.*
- *Sabotaje informático (303 b). Destrucción de elaboración de datos de especial significado por medio de destrucción, deterioro, Inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.*
- *Utilización abusiva de cheques o tarjetas de crédito (art. 266b)".*[57]

Estas disposiciones entraron en vigencia en virtud que la estafa informática, empezó a ganar terreno peligrosamente y en niveles alarmantes en el país Europeo, lo que determino la urgencia de formular una nueva normativa penal que sancione este tipo de ilícitos.

Las diversas formas de aparición de la criminalidad informática propician además, la aparición de nuevas lesiones de bienes jurídicos merecedoras de

[57] ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador.

pena, en especial en la medida en que el objeto de la acción puedan ser datos almacenados o transmitidos o se trate del daño a sistemas informáticos. El tipo de daños protege cosas corporales contra quebrantos de su sustancia o función de alteraciones de su forma de aparición.

4.4.2. Austria

En Austria también se evidencio un cambio en el tratamiento de las infracciones y delitos informáticos, es así que se promulgo la Ley Reformatoria del Código Penal, del 22 de diciembre de 1987, contemplado los siguientes delitos:

- *¨Destrucción de datos (Art. 126). En este artículo se regulan no solo los datos personales sino también los no personales y los programas.*
- *Estafa informática (Art. 148). En este artículo se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el curso del procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.¨*[58]

Con la entrada en vigencia de estas reformas, se pudo penalizar a la estafa informática, en la cual exista un perjuicio económico a terceros. En la cual se puntualiza, que este tipo de perjuicios puede ser a través de todo tipo de

[58]ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador.

alteración de datos. Recalcando como agravante sanciones a los que utilicen sus conocimientos o profesión para el cometimiento.

4.4.3. Francia

Con el boom tecnológico no se expendieron únicamente los adelantos para bien sino que, también se utilizaron estas innovaciones para el causar perjuicio a las personas, es por ello que para contrarrestar esta situación los legisladores franceses debatieron e implementaron Ley número 88-19 el 5 de enero de 1988 sobre el fraude informático, en la cual se tomaron en consideración aspectos fundamentales en el Código Penal como:

- *¨Acceso fraudulento a un sistema de elaboración de datos (Art. 462-2). - En este artículo del se sanciona tanto el acceso al sistema como al que se mantenga en él y aumenta la sanción correspondiente si de ese acceso resulta la supresión o modificación de los datos contenidos en el sistema o resulta la alteración del funcionamiento del sistema.*
- *Sabotaje informático (Art. 462-3). - En este artículo del se sanciona a quien impida o falsee el funcionamiento de un sistema de tratamiento automático de datos.*
- *Destrucción de datos (Art. 462-4). - En este artículo del se sanciona a quien intencionadamente y con menosprecio de los derechos de los demás introduzca datos en un sistema de tratamiento automático de datos o suprima o modifique los datos que este contiene o los modos de tratamiento o de transmisión.*

- *Falsificación de documentos informatizados (Art. 462-5). - En este artículo se sanciona a quien de cualquier modo falsifique documentos informatizados con intención de causar un perjuicio a otro.*
- *Uso de documentos informatizados falsos (Art. 462-6) En este artículo se sanciona a quien conscientemente haga uso de documentos falsos haciendo referencia al artículo 462-5.*[59]

La legislación francesa, amplio mucho el panorama, ya que tomo en consideración varios aspectos que caracterizaban el cometimiento de la infracción es por ello que se normo desde los siguientes aspectos, Acceso fraudulento a un sistema de elaboración de datos, Sabotaje informático, Destrucción de datos, Falsificación de documentos informatizados, lo que permitió que varias legislaciones, vayan innovando y penalizando dándole ya categorías y tipificando según las características de la infracción.

4.4.4. Estados Unidos.

En los Estados Unidos ya hace algunos años atrás se empezó a tratar estos asuntos, muestra de ello es la creación del Acta de Fraude y Abuso Computacional suscrita en el año de 1986.

Como esta Acta no cumplió con las expectativas trazadas en 1994, se adopta el Acta de Abuso Computacional, cuya finalidad era eliminar la

[59]ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador.

transmisión de programas, información, códigos o comandos que causan daños a la computadora, al sistema informático, a las redes, información, datos o programas.

Esta Acta de 1994, evoluciono la legislación sobre estos aspectos ya que regulo el uso tecnológico con el fin de lanzar ataques de virus, con el propósito de causar daños a las personas.

¨El acta define dos niveles para el tratamiento de quienes crean virus estableciendo para aquellos que intencionalmente causan un daño por la transmisión de un virus, el castigo de hasta 10 años en prisión federal más una multa y para aquellos que lo transmiten solo de manera imprudencial la sanción fluctúa entre una multa y un año en prisión.

En opinión de los legisladores estadounidenses, la nueva ley constituye un acercamiento más responsable al creciente problema de los virus informáticos, específicamente no definiendo a los virus sino describiendo el acto para dar cabida en un futuro a la nueva era de ataques tecnológicos a los sistemas informáticos en cualquier forma en que se realicen. Diferenciando los niveles de delitos, la nueva ley da lugar a que se contemple qué se debe entender como acto delictivo".[60]

Esto motivo a que se realicen cambios sustanciales en la Sección 502 del Código Penal en lo que tiene que ver a los delitos informáticos en las que se ampliaron las sanciones pecuniarias por persona afectada, cuyo objetivo era el de aumentar la protección a las personas, negocios y dependencias gubernamentales, del uso fraudulento de la tecnología para interferir, dañarlo acceder a bases de datos y sistemas computarizados creados legalmente.

[60]ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador.

4.4.5. Chile

Una vez que he presentado un análisis de países Europeos y de Norte América, es momento de referirnos a países ubicados en la región sur del continente, en donde para mi modesto parecer la legislación chilena ha sido pionera en la transformación de la justicia en los aspectos materia de la presente investigación.

A mediados del año 1993 entró en vigencia en Chile la Ley N°19.223, la cual se refería explícitamente a delitos informáticos, con categoría de ley especial, extra código y consta de 4 artículos, que me permitiré transcribir a continuación:

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

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

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

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

Artículo 4. El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio. Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado¨.[61]

Esta ley aborda el tema desde los aspectos del sabotaje y del espionaje, dependiendo del daño o perjuicio provocado se aplicó las penalidades así por ejemplo, en el caso de que alguien destruya dolosamente un computador, podía recibir como castigo la pena de prisión menor en su grado medio a máximo, desde 541 días hasta 5 años de cárcel, en el caso de que un hacker, por ejemplo, ingresa indebidamente a un sistema para conocer información sin autorización, puede recibir desde 61 días hasta 3 años de presidio.

Esas sanciones vienen a categorizar de cierta manera a la infracción, y determinan las escalas que se podrían aplicar al momento de sancionar con el fin de que sea acorde la infracción o delito con la pena o sanción que se le imponga al autor a autores.

[61]ACURIO, del Pino, Santiago, Delitos Informáticos. Quito- Ecuador.

5 MATERIALES Y METODOS

En la realización de la presente Tesis, utilice los distintos métodos que nos presenta la investigación, tales como métodos inductivo, deductivo, analítico y sintético, además utilice diferentes procedimientos y técnicas que la investigación científica proporciona y que permiten descubrir, sistematizar, y ampliar todos aquellos nuevos conocimientos adquiridos en el proceso.

5.1 METODOS

El presente trabajo de tesis me regí de manera principal por el método científico que implico definir un conjunto de procedimientos orientados a la obtención de conocimientos científicos.

Tome como referencia inicial la Constitución de la República del Ecuador, el Código Penal, y el Derecho Comparado con la finalidad de definir las características, que se presentan en las infracciones informáticas, así como analizar las sanciones existentes en otras legislaciones.

Para señalar los principales métodos utilizados tenemos los siguientes:

5.5.1. MÉTODO HIPOTÉTICO-DEDUCTIVO

Con el análisis de jurisprudencia, leyes y doctrina, es decir mediante procedimientos inductivos y deductivos, en su momento, he presentado un proyecto de ley reformatoria al Código Penal tendiente a regular el marco sancionar de las infracciones informáticas en la legislación ecuatoriana.

5.5.2. MÉTODO LÓGICO DEDUCTIVO

Utilizado para el análisis de las disposiciones constitucionales, legales, derecho comparado, doctrina y jurisprudencia, llegue a establecer las diferencias existentes en el marco sancionador de las infracciones informáticas, en las diferentes legislaciones y de manera particular en la legislación ecuatoriana.

5.1.3. MÉTODO LÓGICO INDUCTIVO

Partí de casos reales que en primer lugar me permitieron palpar la realidad, pudiendo determinar las necesidades y los requerimientos que se presentan en el campo en si del ejercicio profesional, para llegar a obtener conocimientos generales.

Debiendo recalcar que no se realizará una inducción general si no de muestreo, toda que resultaría imposible tomar la totalidad de casos en los que se han presentado infracciones informáticas, por lo que se utilizó una muestra que nos acerque a la realidad en la cual se desenvuelven los

procesos en las diferentes cortes provinciales de justicia del país, en el cual están en juego diferentes derechos de las personas, en los cuales la norma tiene que establecer la horizontalidad y la imparcialidad.

5.2.- TÉCNICAS

Para la realización de este trabajo de tesis, considerando su naturaleza, se utilizó básicamente la técnica de la observación, con la finalidad de obtener la mayor cantidad de información y saber la forma en que se sancionan las infracciones informáticas en la legislación ecuatoriana, determinando si son efectivas las sanciones existentes o si es necesaria una reforma.

Las técnicas utilizadas para el desarrollo de la investigación de campo de la presente tesis fueron la encuesta, con la cual se pudo obtener una apreciación general del criterio de los Abogados en libre ejercicio profesional; y la entrevista para lo obtención de información especializada, está tomada del criterio de los Jueces de Garantías Penales y Fiscales de la Provincia del Azuay.

6.- RESULTADOS

6.1. ANÁLISIS, PRESENTACIÓN DE LOS RESULTADOS DE LA ENCUESTAS.

En la presente tesis, se realizó la recolección de la información de campo a través de la encuesta la misma que se la aplico a un número de treinta Abogados de libre ejercicio profesional de la ciudad de Cuenca, quienes han expuesto sus criterios sobre las infracciones informáticas, el marco sancionador y más situaciones relacionadas de manera directa con la temática.

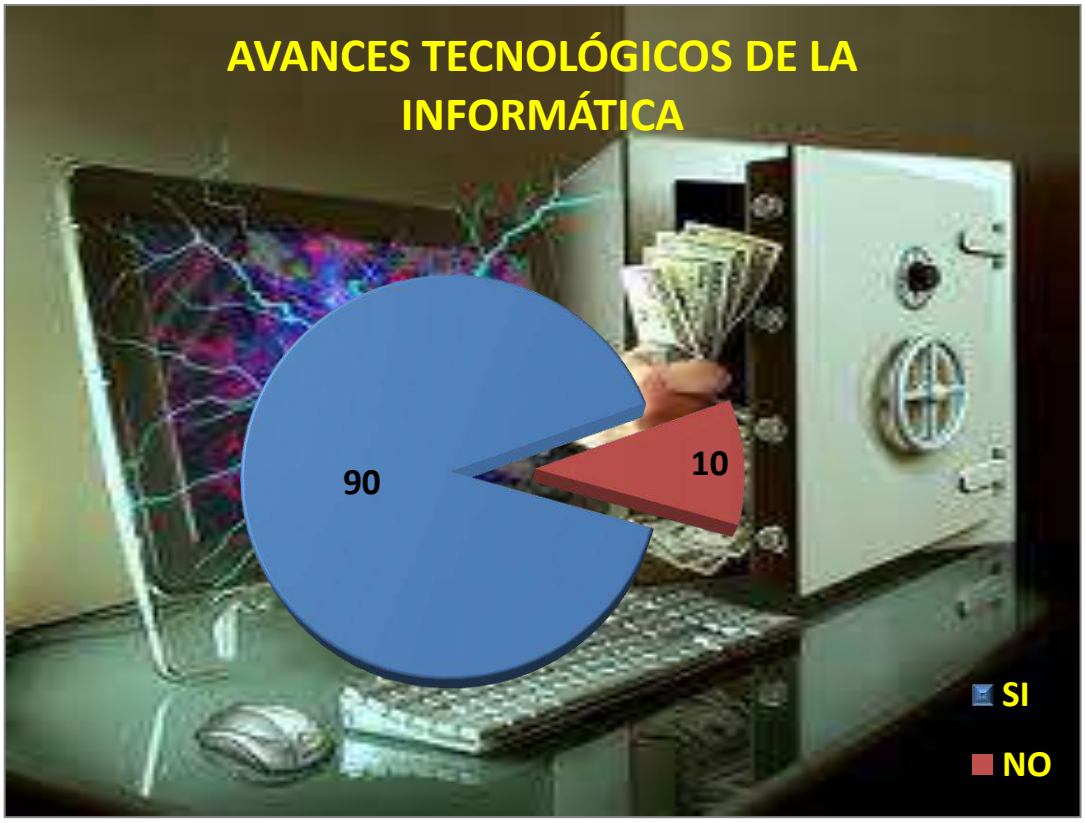
La encuesta fue diseñada y elaborada tomando en consideración la problemática, los objetivos y la hipótesis planteada, de la cual se pudieron establecer siete interrogantes:

1. ¿Conoce usted los avances tecnológicos de la Informática?

CUADRO Nº 1

INDICADORES	FRECUENCIA	PORCENTAJE %
SI	27	90 %
NO	3	10 %
TOTAL	**30**	**100 %**

GRAFICO 1



FUENTE: Abogados en libre ejercicio.
ELABORACIÓN: Luis Pablo Méndez Vanegas

ANÁLISIS:

De acuerdo a la primera interrogante, puedo manifestar que de los 30 encuestados, 27 de ellos responden que si conocen los avances tecnológicos de la informática, lo que representa el 90%; y 2 de ellos manifiestan que desconocen los avances tecnológicos de la informática, lo que representa el 10% del total de la muestra.

INTERPRETACIÓN

En la presente interrogante tenemos un resultado mayoritario por la opción afirmativa, manifestándonos que son evidentes los avances tecnológicos que se presentan día a día, avances que se están incorporando a cada una de las profesiones como herramientas de trabajo, estos avances se presentan a través de los diferentes medios de comunicación y sobre todo en la puesta en venta los diferentes equipos electrónicos de última generación, los cuales se caracterizan por sus pequeños tamaños y su multifuncionalidad, un grupo minoritario desconoce en si los avances tecnológicos que ha sufrido la informática, denotando que es un grupo bastante tradicionalista que por la costumbre son reacios a la utilización de las nuevas tecnologías, motivo por el cual muestran su desinterés por conocer de ellos.

2. ¿Sabe usted que mediante la informática se puede cometer infracciones?

CUADRO Nº 2

INDICADORES	FRECUENCIA	PORCENTAJE %
SI	21	70 %
NO	9	30 %
TOTAL	**30**	**100 %**

GRAFICO 2

FUENTE: Abogados en libre ejercicio.
ELABORACIÓN: Luis Pablo Méndez Vanegas

ANÁLISIS:

De acuerdo a la segunda interrogante, puedo manifestar que de los 30 encuestados, 21 de ellos responden que conocen de que mediante la utilización herramientas informáticas se pueden cometer infracciones, lo que representa el 70%, otro grupo considerable esto es 9de los encuestados responden que desconocen que se puedan cometer infracciones mediante herramientas informáticas, lo que corresponde al 30% de la muestra.

INTERPRETACIÓN

El criterio de los encuestados, se inclina de forma mayoritaria por determinar que efectivamente la informática y sus avances han servido para innovar y desarrollar diferentes sistemas en beneficio de las personas, pero que es indudable de que también esta tecnología ha sido utilizada por personas inescrupulosas para intentar perjudicar a otras o para beneficiarse en perjuicio de otras lo que se consideran infracciones informáticas, un grupo de los encuestados señala que es muy difícil que se den este tipo de infracciones pero sin manifestar hechos categóricos que puedan respaldar su tesis u opinión lo que dificulta poder desarrollar un mejor análisis de su opinión.

3. ¿Conoce usted que si la Legislación Ecuatoriana sanciona este tipo de delitos?

CUADRO Nº 3

INDICADORES	FRECUENCIA	PORCENTAJE %
SI	18	60 %
NO	12	40 %
TOTAL	**30**	**100 %**

GRAFICO 3

FUENTE: Abogados en libre ejercicio.
ELABORACIÓN: Luis Pablo Méndez Vanegas

ANÁLISIS:

De acuerdo a la tercera interrogante, puedo manifestar que de los 30 encuestados, 18 manifiestan conocer que en la Legislación Ecuatoriana se sanciona este tipo de infracciones, lo que representa el 60%, mientras que un grupo considerable de encuestados, esto es 12 de los encuestados, responden que no están reguladas en nuestra legislación de forma clara las sanciones para este tipo de infracciones, que representa el 40% del total de la muestra, criterio que abre las puertas a un análisis más amplio.

INTERPRETACIÓN

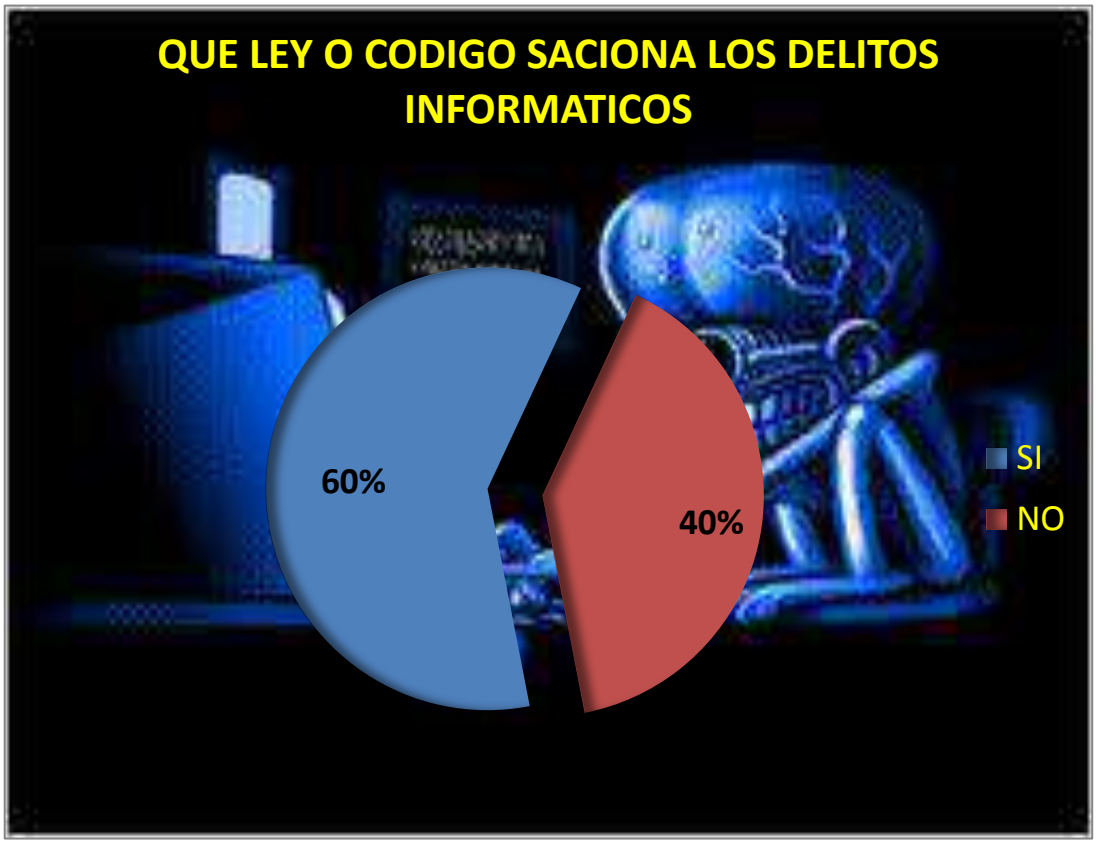
En esta interrogante la mayoría de los encuestados manifiestan que la en la actualidad el Código Penal sanciona este tipo de infracciones y que a mas de ello existe la Ley de Comercio electrónico, firmas electrónicas y mensajes de datos que también ayuda a la regulación en estos aspectos, pero recalcando que de forma principal las infracciones informáticas son sancionadas por el Código Penal, un grupo considerable de los encuestados manifiesta que no se encuentra especificado de forma clara las sanciones para las infracciones informáticas, manifestando que es una conducta delictiva nueva, que sus casos no son frecuentes o que al menos no han sido públicos, motivo por el cual no existen mayores datos para aportar sobre este asunto.

4. ¿Conoce usted que Ley o Código, sanciona las Infracciones Informáticas?

CUADRO Nº 4

INDICADORES	FRECUENCIA	PORCENTAJE %
SI	18	60 %
NO	12	40 %
TOTAL	**30**	**100 %**

GRAFICO 4



FUENTE: Abogados en libre ejercicio.
ELABORACIÓN: Luis Pablo Méndez Vanegas

ANÁLISIS:

De acuerdo a la cuarta interrogante, los encuestados se pronunciaron de la siguiente manera de 30 encuestados, 18 responden que si conocen que cuerpo legal sanciona las infracciones informáticas; lo que representa el 60%, mientras que 12 de ellos consideran que esta claro el marco sancionador en nuestra legislación por lo que se abstienen de pronunciarse, lo que representa el 40% del total de la muestra.

INTERPRETACIÓN:

Los encuestados de manera mayoritaria se pronuncian por que si conocen el marco sancionador de las infracciones informáticas, al solicitar la ampliación a su respuesta esta es retroalimentada con el pronunciamiento de que el Código Penal es el cuerpo legal que sanciona todo tipo de delitos en los cuales dentro de su articulado también se refiere a los delitos informáticos, de los cuales si bien es cierto no existe un amplio tratamiento pero existe un marco sancionador, el resto de encuestados se inclinan por la opción negativa manifestando que no conocen que cuerpo legal trata este tipo de infracciones, ratificando su pronunciamiento en la pregunta anterior.

5. ¿Sabe usted en que forma la Legislación Ecuatoriana sanciona a las personas que cometen Infracciones Informáticas?

CUADRO Nº 5

INDICADORES	FRECUENCIA	PORCENTAJE %
SI	12	40 %
NO	18	60 %
TOTAL	**30**	**100 %**

GRAFICO 5

FUENTE: Abogados en libre ejercicio.
ELABORACIÓN: Luis Pablo Méndez Vanegas

ANÁLISIS:

De acuerdo a la quinta interrogante, manifiesto que de los 30 encuestados, 18 responden que no conocen la forma en que se sancionan las infracciones informáticas en la legislación ecuatoriana, lo que representa el 60%, mientras que 12 de ellos determinan que si conocen la forma de sanción a las infracciones informáticas, lo que representa el 40% de la muestra.

INTERPRETACIÓN:

La mayoría de los encuestados manifiestan que no saben cómo se sancionan específicamente en el Código Penal a las infracciones informáticas, lo que nos demuestra que existe mucho desconocimiento sobre el tratamiento que nuestra legislación da a este tipo de infracciones, lo que a lo mejor puede contribuir a que poco se hable del tema, mientras que un porcentaje inferior pero considerable saben las sanciones que determina el Código Penal a las infracciones informáticas, las cuales van desde seis meses a nueve anos de prisión y multas económicas que pueden llegar hasta los diez mil dólares, y en sus comentarios manifiestan que no se le ha dado la importancia del caso a este tema motivo por el cual para muchos les parece nuevo pero existente.

6. ¿Considera usted que las sanciones aplicadas a las personas que cometen Infracciones Informáticas, guardan relación con el perjuicio que causan a las víctimas?

CUADRO Nº 6

INDICADORES	FRECUENCIA	PORCENTAJE %
SI	12	40 %
NO	18	60 %
TOTAL	**30**	**100 %**

GRAFICO 6

FUENTE: Abogados en libre ejercicio.
ELABORACIÓN: Luis Pablo Méndez Vanegas

ANÁLISIS:

En la sexta interrogante, manifiesto que de los 30 encuestados, 18 responden que no conocen la forma en que se sancionan las infracciones informáticas en la legislación ecuatoriana, lo que representa el 60%, mientras que 12 de ellos determinan que si conocen y determinan que no se relacionan las penas a los perjuicios, lo que representa el 40% de la muestra.

INTERPRETACIÓN:

La mayoría de los encuestados se pronuncian de forma negativa debido a que no saben cómo se sancionan específicamente en el Código Penal a las infracciones informáticas, el grupo de jurisconsultos que conocen sobre el tema y están más empapados en él se manifiestan indicando que si bien es cierto que el Código Penal ya incluye sanciones para este tipo de infracciones, estas no guardan relación a los daños que puedan ocasionar, y sobre todo que los administradores de justicia siempre aplica las mínimas, lo que provoca impunidad y que siga el auge de infracciones utilizando herramientas informáticas.

7. ¿Considera usted que se debe Reformar el Código de Procedimiento Penal tendiente a endurecer las sanciones al cometimiento de las infracciones informáticas, procurando que estas sanciones guarden estrecha relación con el perjuicio causado a las víctimas?.

CUADRO Nº 7

INDICADORES	FRECUENCIA	PORCENTAJE %
SI	21	70 %
NO	9	30 %
TOTAL	**30**	**100 %**

GRAFICO 7

FUENTE: Abogados en libre ejercicio.
ELABORACIÓN: Luis Pablo Méndez Vanegas

ANÁLISIS:

De acuerdo a la última interrogante, puedo manifestar que de los 30 encuestados, 21 de ellos que están de acuerdo con la reforma al Código Penal con el fin de que las sanciones guarden relación al perjuicio ocasionado, lo que representa el 70%, otro grupo considerable esto es 9de los encuestados responden que no están de acuerdo con la reforma y que lo legislado hasta el momento es suficiente, lo que corresponde al 30% de la muestra.

INTERPRETACIÓN

El criterio de los encuestados, se inclina de forma mayoritaria por la opción de que es necesario presentar un Proyecto de Reforma tendiente a endurecer las sanciones al cometimiento de las infracciones informáticas, procurando que estas sanciones guarden estrecha relación con el perjuicio causado a las víctimas, manifestando que solo de esta manera se podrá erradicar este tipo de delincuencia que cada día intenta utilizar nuevas técnicas o herramientas para perjudicar a los ciudadanos, el grupo de minoría y que a lo largo de la presente encuesta han mantenido un criterio conservador y reacios a reconocer los avances que la tecnología y la informática precisamente nos presenta manifiestan que no es necesaria una reforma al Código Penal señalando que la legislación o normativa vigente es suficiente.

Es necesario señalar que luego de los resultados de la presente encuesta existen dos tipos de Abogados en libre ejercicio, un grupo tradicionalista reacios a reconocer los cambios que se presentan y un grupo de nuevos Abogados o Abogados jóvenes que están conscientes de los cambios y sobre todo con los cambios que se deben presentar a los diferente cuerpos legales con el fin de que estos respondan a la necesidad real y actual de una correcta administración de justicia, en beneficio exclusivo de los habitantes que constantemente están siendo víctimas de estas infracciones..

7. DISCUSIÓN

Una vez que he concluido la investigación literaria y la recopilación de la información de campo, se puede llegar a establecer y determinar si se han cumplido los siguientes objetivos tanto generales como específicos que fueron planteados en el proyecto de tesis, además realizar la contratación de hipótesis, para pasar a presentar la fundamentación jurídica a la propuesta de reforma legal.

7.1. VERIFICACION DE OBJETIVOS

Objetivo General:

Realizar un estudio Jurídico, Crítico y Doctrinario, sobre las Infracciones Informáticas en la Legislación Penal Ecuatoriana.

Este objetivo se cumplió en su totalidad, de manera particular en el desarrollo de la revisión de literatura, inicialmente en el marco conceptual ya que se da una visión general de diferentes términos de uso frecuente que facilitaron la comprensión de la tesis, posteriormente en el marco doctrinario que permitió realizar un análisis más profundo sobre las infracciones informáticas tomando en consideración los diferentes criterios de varios autores que se han referido en diferentes obras de acuerdo a la temática planteada, y finalmente el marco jurídico y derecho comparado, en virtud de que se presentó a la luz la realidad del tratamiento que da nuestra

legislación a la infracciones informáticas y su comparación con las diferentes legislaciones de otros países relacionadas con el tema.

Objetivos Específicos:

Establecer que los bienes garantizados en la Constitución, tales como la intimidad, se ven afectados al no otorgar una sanción acorde con el delito cometido en materia de delitos informáticos.

Se ha podido comprobar el presente objetivo, con lo expresado por los encuestados, en las preguntas en la sexta y séptima interrogante, que hace referencia sobre que las sanciones determinadas en el Código Penal, a las sanciones informáticas no están acordes a los daños o perjuicios causados, afectando de manera directas bienes jurídicos garantizados por la Constitución de la República como la intimidad, ya que el uso doloso de información causa por lo regular graves perjuicios a la moral, aspectos garantizados incluso por los tratados internacionales reconocidos por el Estado, motivo por el cual se cumple plenamente el objetivo.

Realizar un estudio comparado en legislación penal de otros países, a fin de establecer la correlación con la legislación penal ecuatoriana, en materia de delitos informáticos.

Este objetivo se cumplió en su totalidad con el análisis de la Legislación Comparada ya que con este análisis podemos apreciar de manera general la forma en que se juzgan y sancionan este tipo de infracciones informáticas en otros países, y que han servido de referente para que nuestra legislación adopte este tipo de medidas con el fin de garantizar la protección de los derechos de las personas. Este análisis lo realice tomando en consideración las más representativas ya que resultaría imposible realizar el análisis de todas las legislaciones que se refieren a la presente temática.

Presentar un Proyecto de Ley Reformatoria al Código Penal con el fin de castigar severamente a las personas que cometan Infracciones Informáticas.

De lo expuesto en la presente tesis, los resultados de la investigación de campo, determinan los criterios de los encuestados y entrevistados que en la séptima interrogante hacen referencia a la necesidad imperiosa de reformar el Código Penal tendiente a sancionar severamente las infracciones informáticas, ya que estas pueden ocasionar incalculables perjuicios económicos y morales a las víctimas, atentando a bienes jurídicos garantizados por la Constitución de la República del Ecuador.

7.2. CONTRASTACIÓN DE LA HIPÓTESIS

La benevolencia de las sanciones a las Infracciones Informáticas en la Legislación Ecuatoriana ha provocado el incremento de los actos delictivos, haciendo uso de herramientas tecnológicas de fácil acceso para los ciudadanos.

Con todo lo anteriormente señalado puedo determinar que se ha contrastado la hipótesis inicialmente planteada ya que el criterio de los Abogados en libre ejercicio profesional es categórico en manifestar que las penas que se aplican actualmente a las infracciones informáticas, son benevolentes, motivo por el cual se han incrementado considerablemente el cometimiento de este tipo de delitos.

7.3. FUNDAMENTOS JURÍDICOS DE LA PROPUESTA DE REFORMA LEGAL.

En el Libro Segundo del Código Penal TITULO II, DE LOS DELITOS CONTRA LAS GARANTIAS CONSTITUCIONALES Y LA IGUALDAD RACIAL, en el CAPITULO V, De los delitos contra la inviolabilidad del secreto, en su Art. 202 A, se determina:

"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, será sancionada 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 realiza 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"[62].

A continuación el Código Penal en su Art. 202 B) determina:

"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."[63]

En el Título III del libro anteriormente señalado se hace referencia a LOS DELITOS CONTRA LA ADMINISTRACION PUBLICA, Capítulo V, De la Violación de los deberes de Funcionarios Públicos, de la Usurpación de Atribuciones y de los Abusos de Autoridad, y en su Art. 262 señala:

"Serán reprimidos con tres 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,

[62] Código Penal, Ecuatoriano, Art. 202 A.
[63] Código Penal Ecuatoriano Art. 202 B.

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 sin razón de su cargo."[64]

Más adelante en el Titulo IV, DE LOS DELITOS CONTRA LA FE PUBLICA. En su capítulo III, De las Falsificaciones de Documentos en General en su Art. 353 A).

"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.

[64] Código Penal Ecuatoriano Art. 262.

4.- El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.”[65]

En el Titulo V. DE LOS DELITOS CONTRA LA SEGURIDAD PUBLICA. Capítulo VII: del incendio y otras Destrucciones, de los deterioros y daños, en el Art. 415 A) y 415 B) determinan:

“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 seiscientos 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 vinculada con la defensa nacional.”[66]

Art. 415 B. 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

[65] Código Penal Ecuatoriano Art. 353 A
[66] Código Penal Ecuatoriano Art. 415 A

reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica."[67]

[67]Código Penal Ecuatoriano Art. 415B

8. CONCLUSIONES

Luego de culminar la presente tesis, me permito formular las siguientes conclusiones, las mismas que se encuentran apegadas a la realidad investigada, las que a mi juicio abarca todo el proceso.

1. El aspecto más importante de la informática es información, que ha llegado alcanzar un incalculable y valioso valor económico, motivo por el cual su correcto uso puede crear grandes redes de servicios, comercio, educación etc., apoyando al desarrollo de las naciones.

2. Desgraciadamente en todas las circunstancias de las diferentes actividades de los humanos, existe el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva las infracciones y el delito.

3. Todos los adelantos tecnológicos han sido aprovechados por los delincuentes quienes aprovechando de la vulnerabilidad del acceso de información a través de redes de comunicación y más aun con la aparición de la Internet, ha creado comportamientos ilícitos denominados de forma genérica como delitos informáticos, de índole patrimonial y socioeconómica, produciendo innumerables perjuicios a las personas.

4. La Constitución norma máxima y suprema protege la información personal en todos sus aspectos, esta protección consta entre los derechos

de libertad de las personas, es por ello que la información personal es considerada como confidencial y su acceso, divulgación y uso deben estar autorizados por el titular o por el mandato de la Ley, la violación a ello constituye un delito que podría causar daños irreparables.

5. En el Libro Segundo del Código Penal TITULO II, DE LOS DELITOS CONTRA LAS GARANTIAS CONSTITUCIONALES Y LA IGUALDAD RACIAL, en el CAPITULO V, De los delitos contra la inviolabilidad del secreto, en su Art. 202 A, se determina que, 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…",estableciendo además algunas circunstancias que agravan las sanciones, pero resultan leves para la gravedad de la infracción cometida, siendo necesario que se castigue severamente estas conductas, motivo por el cual es imperiosa la presentación de un proyecto de reforma al Código Penal.

9. RECOMENDACIONES.

Luego de finalizar el desarrollo dela presente tesis he creído conveniente, formular las recomendaciones siguientes:

1. Al Poder Ejecutivo, al momento de autorizar la introducción en el mercado de nuevas tecnologías se deben exigir las medidas necesarias con el fin de que los usuarios de ellas no puedan ser presa de la delincuencia, por la vulnerabilidad de sus sistemas.

2. A usuarios, consumidores y ciudadanía en general, al momento de ser perjudicados por infracciones informáticas, presentar las denuncias respectivas ante las Autoridades competentes con el fin de que se sancionen a los culpables evitando queden estos casos en la impunidad y que las Autoridades conozcan la forma de operar de los delincuentes para poder tomar acciones para evitar su cometimiento.

3. A las Universidades del país, preferentemente aquellas creadoras de ciencia y tecnología incentivar el desarrollo y creación de mecanismos de seguridad para evitar la vulnerabilidad de los sistemas informáticos.

4. A la Asamblea Nacional, emprender en el tratamiento de un proyecto de Ley Reforma al Código Penal, tendiente sancionar severamente las infracciones informáticas, y sobre todo que las sanciones guarden estrecha relación con el perjuicio causado a las víctimas.

5. Al Consejo Nacional de la Judicatura, levantar bases estadísticas sobre las formas de cometimiento de las infracciones informáticas, las cuales servirán para realizar campañas de información y prevención para evitar el incremento de estas infracciones.

9.1. PROPUESTA JURIDICA

LA ASAMBLEA NACIONAL

LA COMISIÓN DE LEGISLACIÓN Y CODIFICACIÓN

CONSIDERANDO:

Que, el numeral 9 del artículo 11 de la Constitución de la República del Ecuador, publicada en el Registro Oficial No. 149 de 20 de octubre de 2008 determina que el más alto deber del Estado consiste en respetar y hacer respetar los derechos garantizados en la Constitución de la República del Ecuador.

Que, el Art. 66 de la Constitución de la República del Ecuador garantiza el derecho a la intimidad personal y familiar.

Que, el artículo 169 de la Constitución de la República del Ecuador, dispone que el sistema procesal es un medio para la realización de la justicia. Las normas procesales consagrarán los principios de simplificación, uniformidad, eficacia, inmediación, celeridad y economía procesal, y harán efectivas las garantías del debido proceso. No se sacrificará la justicia por la sola omisión de formalidades.

Que, en ejercicio de sus facultades constitucionales y legales constantes en el artículo 120, numeral 6, expide la siguiente:

LEY REFORMATORIA AL CÓDIGO PENAL.

Art. 1.- **SUSTITUYASE,** los Artículos 202 A, 202 B) por los siguientes

Art. 202 A.- 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 uno a dos años y multa de mil a dos 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 tres a seis años de prisión y multa de dos mil a cuatro mil 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 cuatro a ocho años y multa de cinco mil a veinte 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 diez mil a veinte mil dólares de los Estados Unidos de Norteamérica.

Art. 202 B.- 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 seis meses a cuatro años y multa de dos a cinco mil dólares de los Estados Unidos de Norteamérica."

DISPOSICIÓN FINAL:

Esta ley entrará en vigencia a partir de su publicación en el Registro Oficial.

Dado y suscrito en la sede de la Asamblea Nacional, ubicada en el distrito Metropolitano de Quito, a los treinta días del mes de octubre del dos mil doce.

…… ……

Presidente de la Asamblea Nacional Secretario General

10. BIBLIOGRAFIA

1. AGUIRRE, Guzmán, Vanessa, Nulidades en el Proceso Civil.

2. BELLUSCIO Claudio, Abogado, Derecho de Familia, Infancia y Adolescencia, Facultad de Derecho de la UCE, Quito-Ecuador, Año 2009.

3. CABANELLAS, de Cuevas Guillermo, Diccionario Jurídico Elemental, Editorial Heliasta, Buenos Aires Argentina.

4. CARRILLO, Castellanos, Enoe, CITACIONES Y NOTIFICACION.

5. Código Civil Ecuatoriano, Corporación de Estudios y Publicaciones.

6. Código de Procedimiento Civil Ecuatoriano, Corporación de Estudios y Publicaciones.

7. CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR, Corporación de Estudios y Publicaciones, Junio 2009.

8. COUTURE, Eduardo, J., Fundamentos del derecho Procesal Civil

9. ERAZO LEDESMA, Gonzalo, Tratado de las Instituciones del Código Civil, Universidad Nacional de Loja, año 2006.

10. Espasa Calpe, S.A ., Madrid 1991

11. GARCIA, Falconi, José, La citación con la demanda, 2010.

12. GAY, José, Diccionario Enciclopédico Nuevo Océano, Editorial Océano, Barcelona España

13. GOLDSTEIN, Mabel, Diccionario jurídico, Consultor Magno, Panamericana formas e impresos S.A. Bogotá, Colombia, 2008.

14. LARREA HOLGUIN, Juan, Derecho Civil del Ecuador, cuarta edición, Corporación de Estudios y Publicaciones, Quito, año 1985.

15. OSORIO, Manuel, diccionario de Ciencias Jurídicas Políticas y Sociales.

16. http://es.wikipedia.org/wiki/Pensi%C3%B3n_alimenticia. 15/12/2011

17. www.derechoshumanos/Convención de los Derechos del Niño en las Relaciones de Familia/org.com

18. [1]http://es.wikipedia.org/wiki/Citaci%C3%B3n 10/12/2011.

19. http://es.wikipedia.org/wiki/Medio_de_comunicaci%C3%B3n 21/01/2012.

20. http://co106w.col106.mail.live.com/default.aspx?wa=wsignin1.0#!/mail/InboxLight.aspx?n 21/12/2012

11. ANEXOS

UNIVERSIDAD NACIONAL DE LOJA

MODALIDAD DE ESTUDIOS A DISTANCIA

CARRERA DE DERECHO

TEMA

"REFORMAS EN CUANTO A CASTIGAR SEVERAMENTE LAS INFRACCIONES INFORMÁTICAS EN LA LEGISLACIÓN PENAL ECUATORIANA"

PROYECTO DE TESIS PREVIO A LA OBTENCION DEL TITULO DE ABOGADO

AUTOR

LUIS PABLO MENDEZ VANEGAS

LOJA-ECUADOR

2011

1.- EL TEMA.

“REFORMAS EN CUANTO A CASTIGAR SEVERAMENTE LAS INFRACCIONES INFORMÁTICAS EN LA LEGISLACIÓN PENAL ECUATORIANA”

2.- PROBLEMÁTICA.

Para empezar analizar este problema tenemos que partir por considerar que el aspecto más importante de la informática es información, que ha llegado alcanzar un gran valor económico, el correcto uso de esta información, puede crear grandes redes de servicios, comercio, educación etc., apoyando al desarrollo de los pueblos, pero desgraciadamente, tal como lo señala Luis Camacho Losa, en su publicación El delito Informático, *"en todas las facetas de la actividad humana, existe el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva el delito",* en los últimos años los delincuentes se han aprovechado de la vulnerabilidad del acceso de información a través de redes de comunicación y más con la aparición de Internet, ha creado comportamientos ilícitos denominados de forma genérica como delitos informáticos, de índole patrimonial y socioeconómico, produciendo innumerables perjuicios a las personas.

Ahora bien nuestra legislación aborda de alguna manera esta problemática es así que la Constitución de la República del Ecuador al referirse a los Derechos de libertad en su Art. 66 numerales 19 y 20 establece:

¨19. El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento,

distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley.

20. El derecho a la intimidad personal y familiar.¨

La Constitución norma máxima y suprema protege la información personal en todos sus aspectos, esta protección consta entre los derechos de libertad de las personas, es por ello que la información personal es considerada como confidencial y su acceso, divulgación y uso deben estar autorizados por el titular o por el mandato de la Ley, la violación a ello constituye un delito que podría causar daños irreparables.

En el Libro Segundo del Código Penal TITULO II, DE LOS DELITOS CONTRA LAS GARANTIAS CONSTITUCIONALES Y LA IGUALDAD RACIAL, en el CAPITULO V, De los delitos contra la inviolabilidad del secreto, en su Art. 202 A, se determina que:

*"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…",*estableciendo además algunas circunstancias que agravan las sanciones, pero resultan leves para

la gravedad de la infracción cometida, siendo necesario que se castigue severamente estas conductas.

Todas estas manifestaciones de actos delictivos se presentan a través de fraudes, producidos introduciendo datos falsos, manipulando datos de entrada o salida del computador, clonando tarjetas de débito o crédito, con la finalidad de producir o lograr movimientos falsos en transacciones de una institución o Empresa

Las formas para acceder a este tipo de sistemas han sido variadas y cada vez se perfeccionan más los mecanismos, es por ello que el marco sancionador en la legislación ecuatoriana debe ser mucho más drástico, porque la legislación existente, está permitiendo que cada vez se incrementen este tipo de delitos, ya que quedan fácilmente en la impunidad y en el mejor de los casos cuando se ha llegado a sancionar al poco tiempo los autores nuevamente cometen estas infracciones.

Por todo lo señalado, el proyecto que se ha elaborado está orientado a la necesidad urgente de reforma con el fin de frenar estos delitos.

3.- JUSTIFICACIÓN.

Una vez que me encuentro culminando mi formación profesional en la Carrera de Derecho de la Modalidad de Estudios a Distancia de la Universidad nacional de Loja, es de suma importancia que como futuro profesional del Derecho, me preocupe por investigar y analizar sobre un problema de actualidad, que afecta a la sociedad en general, para luego del desarrollo de la misma poder presentar alternativas de solución, cumpliendo con la obligación moral de retribuir lo aprendido en los años de formación, en miras de solucionar y transformar los diferentes problemas de la sociedad.

Por la naturaleza de la malla curricular de nuestra carrera es evidente que la solución a los diferentes problemas sociales, las debemos proponer mediante un Proyecto de Ley Reformatoria a la diferente normativa existente en nuestro país, justificando de esta manera desde el punto de vista jurídico la presente investigación, por el análisis que debo realizar a los diferentes cuerpos legales, esto es Códigos, Leyes, Reglamentos, etc.

Desde el punto de vista Académico, el presente trabajo se justifica por cuanto, el Reglamento de Régimen Académico, determina como uno de los principales requisitos para la Graduación en la Carrera, la realización de un trabajo de investigación jurídica, en la cual se analicen los diferentes problemas de la sociedad.

En lo referente a la factibilidad de este estudio, considero que es absolutamente viable, pues por mi campo ocupacional y por mi afición a la lectura, cuento con una amplia gama de bibliografía, así como una formación académica suficiente, y sobre todo poseo los recursos materiales y presupuestarios necesarios para poder culminar con éxito el presente trabajo.

4.- OBJETIVOS.

4.1. OBJETIVO GENERAL.

Realizar un estudio Jurídico, Crítico y Doctrinario, sobre las Infracciones Informáticas en la Legislación Penal Ecuatoriana.

4.2. OBJETIVOS ESPECÍFICOS.

- Establecer que los bienes garantizados en la Constitución, tales como la intimidad, se ven afectados al no otorgar una sanción acorde con el delito cometido en materia de delitos informáticos.
- Realizar un estudio comparado en legislación penal de otros países, a fin de establecer la correlación con la legislación penal ecuatoriana, en materia de delitos informáticos.
- Presentar un Proyecto de Ley Reformatoria al Código Penal con el fin de castigar severamente a las personas que cometan Infracciones Informáticas.

5. HIPÓTESIS.

La benevolencia de las sanciones a las Infracciones Informáticas en la Legislación Ecuatoriana ha provocado el incremento de los actos delictivos, haciendo uso de herramientas tecnológicas de fácil acceso para los ciudadanos.

6.- MARCO TEÓRICO.

Con el pasar del tiempo conforme la sociedad ha ido transformándose y evolucionando, la delincuencia y el crimen organizado no se han quedado atrás de esta evolución, ideándose nuevas formas para cometer sus ilícitos.

Es necesario citar algunos conceptos que facilitaran la comprensión del presente trabajo, es así que en primer lugar determinar el significado de Infracción de la cual Guillermo Cabanellas manifiesta *"Transgresión, quebrantamiento, violación, incumplimiento de una ley, pacto o tratado."* esta pequeña pero concreta definición nos permite conocer que una infracción no es otra cosa que actuar u obrar fuera o en contra de las leyes que rigen a determinado grupo de personas o naciones.

Si actuamos en contra de la Ley, estamos atentando de manera directa contra el resto de personas o sus bienes, determinado esto podemos manifestar que este quebrantamiento obviamente que debe ser ideado, planificado y ejecutado por personas, que se las conoce como Infractor, transgresor, delincuente.

Para cometer este tipo de actos delictivos las personas han utilizado la Tecnología "Conocimientos susceptibles de ser aplicados a la producción de bienes o servicios", con el fin de cumplir sus objetivos esto es aplicando por ejemplo aparatos electrónicos o informáticos como:

1. *Computadores de escritorio o portátiles.*
2. *Servidores que almacenan o transfieren datos electrónicos por internet.*
3. *Teléfonos celulares.*
4. *Aparatos para identificar llamadas.*
5. *GPS, aparato que utiliza el satélite para ubicar a personas o vehículos.*
6. *Cámaras de Video.*
7. *Sistemas de Seguridad, etc.*

Instrumentos que al parecer son inofensivos pero en el momento de que el crimen organizado hace uso de ellos de forma ilícita, pueden provocar severos daños y perjuicios a las personas.

Ahora bien debemos definir al delito informático para lo cual es necesario citar algunos autores es así que:

“Nidia Callegari define al delito informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

Para Carlos Sarzana, los crímenes por computadora comprenden "cualquier comportamiento criminógeno en el cual la computadora ha estado involucrada como material o como objeto de la acción criminógena, como mero símbolo".

María de Luz Lima dice que el "delito electrónico" en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito informático, es cualquier acto ilícito penal, en el

que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".

Los conceptos anteriormente señalados nos permiten deducir elementos comunes: la computadora como medio o fin de la infracción; y, el uso de la informática para el cometimiento de la conducta delictiva.

Por lo tanto, resumiendo, diremos que delitos informáticos son aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio informático.

Todas estas situaciones crean una serie de ciencias que en nuestro medio resultan novedosas para ejemplificar traeré a colación la informática Jurídica la cual *"no es otra cosa que el procesamiento de información jurídica por medios electrónicos, no solo en lo informático, sino en las telecomunicaciones. Es decir el uso de la tecnología en la actividad jurídica."*

Nuestra legislación en algunos tópicos aborda esta problemática motivo por el cual citare las diferentes disposiciones legales relacionadas directamente al tema materia de la presente investigación.

En el Libro Segundo del Código Penal TITULO II, DE LOS DELITOS CONTRA LAS GARANTIAS CONSTITUCIONALES Y LA IGUALDAD RACIAL, en el CAPITULO V, De los delitos contra la inviolabilidad del secreto, en su Art. 202 A, se determina:

"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, será sancionada 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 realiza 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."

A continuación el Código Penal en su Art. 202 B) determina:

"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."

En el Título III del libro anteriormente señalado se hace referencia a LOS DELITOS CONTRA LA ADMINISTRACION PUBLICA, Capítulo V, De la Violación de los deberes de Funcionarios Públicos, de la Usurpación de Atribuciones y de los Abusos de Autoridad, y en su Art. 262 señala:

"Serán reprimidos con tres 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 sin razón de su cargo."

Más adelante en el Titulo IV, DE LOS DELITOS CONTRA LA FE PUBLICA. En su capítulo III, De las Falsificaciones de Documentos en General en su Art. 353 A).

"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.

4.- El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo."

En el Titulo V. DE LOS DELITOS CONTRA LA SEGURIDAD PUBLICA. Capítulo VII: del incendio y otras Destrucciones, de los deterioros y daños, en el Art. 415 A) y 415 B) determinan:

"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 seiscientos 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.

415 B. 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 seiscientos dólares de los Estados Unidos de Norteamérica."

7. METODOLOGÍA.

7.1. Métodos.-El desarrollo de la presente investigación jurídica, está encaminado a realizar un análisis descriptivo y bibliográfico.

La investigación descriptiva es aquella que nos permite descubrir detalladamente y explicar un problema, objetivos y fenómenos naturales y sociales mediante un estudio con el propósito de determinar las características de un problema social.

La investigación bibliográfica consiste en la búsqueda de información en bibliotecas, internet, revistas, periódicos, libros; en las cuales estarán ya incluidas las técnicas de utilización de fichas bibliográficas y nemotécnicas.

La información empírica, se obtendrá de la observación directa de la codificación de otras leyes, el derecho comparado, y en especial del Código de Penal.

Durante esta investigación utilizare los siguientes métodos: El Método Inductivo, Analítico y Científico. El método inductivo, parte de aspectos particulares para llegar a las generalidades es decir de lo concreto a lo complejo, de lo conocido a lo desconocido. El método inductivo en cambio, parte de aspectos generales utilizando el racionamiento para llegar a conclusiones particulares.

El método analítico tiene relación al problema que se va a investigar por cuanto nos permite estudiar el problema en sus diferentes ámbitos. El análisis y síntesis complementarios de los métodos sirven en conjunto para su verificación y perfeccionamiento. El método científico, nos permite el conocimiento de fenómenos que se dan en la naturaleza y en la sociedad, a través de la reflexión comprensiva y realidad objetiva, de la sociedad por ello en la presente investigación me apoyare en este método.

7.2. Técnicas e instrumentos.- En lo que respecta a la fase de la investigación de campo, estará orientada específicamente a las Infracciones Informáticas y su regulación en la Legislación Ecuatoriana, para lo cual se contara con la colaboración de Abogados en Libre Ejercicio, Jueces de Garantías Penales, y Fiscales de Azuay para llegar a determinar un análisis a las encuestas y entrevistas que se realizará en un número de 30 y 5 respectivamente; llegando a prescribir la verificación de los objetivos, de este contenido, me llevará a fundamentar la Propuesta de Ley Reformatoria al Código de Penal, así como el arribo de las conclusiones, recomendaciones.

7.3. Esquema provisional del Informe final.- En cuanto a la presentación del informe final de investigación, me regiré por las normas generales que dicta la metodología de la investigación científica para el efecto, así como por las normas específicas que contempla la Modalidad de Estudios a Distancia en base al Reglamento de Régimen Académico de la Universidad Nacional de Loja, esto es:

PAGINAS PRELIMINARES

I. PORTADA

II. CERTIFICACIÓN DEL DIRECTOR

III. DECLARACIÓN DE AUTORIA

IV. DEDICATORIA

V. AGRADECIMIENTO.

VI. TABLA DE CONTENIDOS:

TABLA DE CONTENIDOS

8. CRONOGRAMA DE TRABAJO.

	AÑO ACADÉMICO 2011					
FASES	**Sep**	**Oct**	**Nov**	**Dic**	**Ene**	**Feb**
	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4	1 2 3 4
Selección del problema	XX					
Elaboración y presentación del proyecto de Investigación.	XX					
Aprobación del Proyecto.		XX				
Elaboración de la teoría de la tesis.		XX	XXX			
Trabajo de campo			X			
Tabulación e interpretación.				X		
Conclusiones				XX		
Recomendaciones					X	
Elaboración del informe definitivo.					X	
Propuesta.					XX	
Aprobación por el Director de Tesis.						X
Reproducción y empastado de Tesis.						X
Disertación, defensa y graduación.						XX

9. PRESUPUESTO Y FINANCIAMIENTO.-

En el presente elemento me permitiré detallar los diferentes recursos a ser utilizados durante de las diferentes fases de la investigación.

9.1 Recursos Humanos.

Postulante: LUIS PABLO MENDEZ VANEGAS

Director de Tesis: Por designarse.

Encuestados: Abogados en libre ejercicio de su profesión.

Entrevistados: Jueces de Garantías Penales.

Fiscales del Azuay.

9.2. Recursos Materiales y Costos.

	DESCRIPCION	COSTOS
1	Adquisición de bibliografía	**$. 450,oo**
2	Útiles de escritorio	**$. 150,oo**
3	Copias Xerox	**$. 50,oo**
4	Internet	**$. 50,oo**
5	Movilización	**$. 300,oo**
6	Impresiones	**$. 100,oo**
7	Empastado	**$. 100,oo**
8	Logística para Sustentación	**$. 100,oo**
9	Imprevistos	**$. 200,oo**
	TOTAL	**$. 1500,oo**

Los costos de la presente investigación jurídica ascienden a la suma de UN MIL QUINIENTOS DOLARES 00/100 USD. 1500,00.

9.3. Financiamiento.

Todos los recursos económicos necesarios para la realización del presente trabajo de investigación jurídica serán financiados con recursos propios del postulante, y con la posibilidad de solicitar Crédito Educativo del IECE o en Una Institución Financiera.

10. BIBLIOGRAFÍA.

1. *ANALUISA LEON, Vicente. "Guía de investigación jurídica MED 2011". Loja- Ecuador. Año 2011.*

2. CABANELLAS, Guillermo, Diccionario de Derecho Usual, Tomo I, Editorial Heliasta, 1990.

3. CAMACHO LOSA, Luis, El Delito Informático, Madrid, España, 1987.

4. CONSTITUCION DE LA REPUBLICA DEL ECUADOR. Corporación de estudios y publicaciones. 2010

5. CODIGO PENAL ECUATORIANO, Corporación de estudios y publicaciones. 2011.

6. PAEZ RIVADENEIRA, Juan José, DERECHO Y NUEVAS TECNOLOGIAS, Corporación de Estudios y Publicaciones. Quito Ecuador. 2010.

7. ZABALA BAQUERIZO, Jorge, Delitos contra la propiedad, Tomo 2, Editorial Edina, Guayaquil Ecuador, 1998.

8. *www.derechoecuador.com.*

UNIVERSIDAD NACIONAL DE LOJA

MODALIDAD DE ESTUDIOS A DISTANCIA

CARRERA DE DERECHO

ENCUESTA

Señores Abogados, sírvase contestar la presente encuesta, su criterio, me permitirá obtener información para realizar mi Tesis de abogado, sobre el tema **"REFORMAS EN CUANTO A CASTIGAR SEVERAMENTE LAS INFRACCIONES INFORMÁTICAS EN LA LEGISLACIÓN PENAL ECUATORIANA".**

1. *¿Conoce usted los avances tecnológicos de la Informática?*

SI ( ) NO ( )

Cuales……
……
……

2. *¿Sabe usted que mediante la informática se puede cometer infracciones?*

SI ( ) NO ( )

Cuales……
……
……

3. *¿Conoce usted que si la Legislación Ecuatoriana sanciona este tipo de delitos?*

SI ( ) NO ( )

¿Por qué
……
……
……

4. *¿Conoce usted que Ley o Código, sanciona las Infracciones Informáticas?*

SI ( ) NO ( )

Cuales……
……
……

5. *¿Sabe usted en que forma la Legislación Ecuatoriana sanciona a las personas que cometen Infracciones Informáticas?*

SI ( ) NO ( )

Cuales……
……
……

6. *¿Considera usted que las sanciones aplicadas a las personas que cometen Infracciones Informáticas, guardan relación con el perjuicio que causan a las víctimas?.*

SI ( ) NO ( )

¿Por qué?
……
……
……

7. *¿Considera usted que existe la necesidad de presentar un Proyecto de Reforma tendiente a endurecer las sanciones al cometimiento de las infracciones informáticas, procurando que estas sanciones guarden estrecha relación con el perjuicio causado a las víctimas?.*

SI ( ) NO ( )

¿Por qué?
……
……
……