UNIVERSIDAD INTERNACIONAL SEK

FACULTAD DE CIENCIAS JURÍDICAS Y SOCIALES

Trabajo de fin de carrera

"ANÁLISIS CRÍTICO DEL TRATAMIENTO JURÍDICO DE LAS TIPOLOGÍAS EN LA LEY PENAL RESPECTO DE LA PROTECCIÓN DE LA INFORMACIÓN INFORMÁTICA EN EL ECUADOR"

Realizado por:

MARIA FERNANDA BASTIDAS PEREZ

Como requisito para la obtención del título de

ABOGADO

QUITO, MAYO 2011

DECLARACIÓN JURAMENTADA

Yo María Fernanda Bastidas Pérez, declaro bajo juramento que el trabajo aquí descrito es de mi autoría, que no ha sido previamente presentada para ningún grado o calificación profesional y que he consultado referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo, a la UNIVERSIDAD INTERNACIONAL SEK, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

…….
María Fernanda Bastidas Pérez

DECLARATORIA

El presente trabajo de investigación de fin de carrera, titulado

"ANÁLISIS CRÍTICO DEL TRATAMIENTO JURÍDICO DE LAS TIPOLOGÍAS EN LA LEY PENAL RESPECTO DE LA PROTECCIÓN DE LA INFORMACIÓN INFORMÁTICA EN EL ECUADOR"

Realizado por la alumna

MARIA FERNANDA BASTIDAS PEREZ

Como requisito para la obtención del título de

ABOGADO

Ha sido dirigido por la profesora

DRA. PAULINA GARCES

Quien considera que constituye un trabajo original de su autor.

……..
Director

Los profesores informantes

DRA. FANNY CORREA
DR. NICOLAS SALAS

Después de revisar el trabajo escrito presentado,
lo han calificado como apto para su defensa oral ante tribunal examinador.

…… …….

DEDICATORIA

A Dios y a la Virgen Dolorosa por ser la guía diaria y constante a lo largo de mi vida.

A mi madre, Ritha, por ser mi amiga, consejera, ayudante y madre, por enseñarme a luchar en cada momento de mi vida, a nunca decaer y que la constancia siempre llevan al éxito.

A mi abuelita, Lucrecia, por ser mi amiga, mi segunda madre, y por su infinito amor y cariño.

A mi padre, Gonzalo, por su apoyo y confianza.

A mi hermana, María Isabel, por su ayuda y credibilidad en este esfuerzo.

A mi abuelito, Sergio, por su constante apoyo y esperanza en mi trabajo.

A mis profesores durante todos mis estudios, porque gracias a ellos aprendí a amar el Derecho, y hacerlo parte fundamental en mi vida.

AGRADECIMIENTO

A mis padres Ritha y Gonzalo por su apoyo y comprensión durante este proceso y gran sueño.

A mis profesores doctores Paulina Garcés, Fanny Correa y Nicolás Salas, por su paciencia y generosidad.

A mis abuelitos, Lucrecia y Sergio, por siempre confiar en mí.

A mi hermana María Isabel, por ser mi ayudante a cada momento en este trabajo.

RESUMEN

Debido a la gran evolución tecnológica que existe actualmente, los delitos en los campos de electrónica e informática también han avanzado, y con esto han generado un daño a las personas que han sido afectadas. Aunque aún este tipo de delitos y su comisión se encuentran un poco ocultos y poco tipificados dentro de nuestra Legislación actual, no por ello dejan de ser graves y peligrosos para las personas que los han sufrido. Actualmente el Código Penal tipifica solamente el daño que existe a la información protegida, es decir la de Bancos, Instituciones públicas y temas de Soberanía Nacional, pero no se encuentra establecido el daño irrogado a la población común y las repercusiones que significa para ellos. Por tanto esto genera que en pleno siglo XXI, y siendo este el siglo de la Era Tecnológica, aún no exista en el Ecuador un avance en relación a este tema.

De esta manera queda demostrado que la Legislación debe ir avanzando a la realidad actual del mundo y con esto los daños que estos fenómenos puedan generar, y a su vez buscar una salida jurídica mediante el acceso a la justicia por medio de los Órganos Jurisdiccionales correspondientes y el respeto a la Ley.

ABSTRACT

Due to the great technological evolution that exists nowadays, the crimes in the fields of electronics and computer science also have advanced, and with this they have generated a hurt to the persons who have been affected. Though still this type of crimes and its commission they are a bit secret and little typified inside our current Legislation, not for it they stop being serious and dangerous for the persons who have suffered them. Nowadays the Penal Code typifies only the hurt that exists to the protected information, that is to say that of Banks, public Institutions and topics of National Sovereignty, but the hurt is not established caused to the common population and the repercussions that it means for them.

Therefore this generates that in full 21st century, and being this the century of the Technological Age, still an advance does not exist in Ecuador in relation to this topic.

Hereby it can only demonstrated that the Legislation must go advancing to the current reality of the world and with this the hurts that these phenomena could generate, and in turn look for a juridical exit by means of the access to the justice by means of the Courts and that this goes of the hand with the Law.

RESUMEN EJECUTIVO

Los delitos informáticos dentro de la sociedad ecuatoriana con el transcurso de los años han evolucionado constantemente, generando con ellos grandes perjuicios a las personas que los sufren, debido a que en la actualidad la informática y el Internet son parte primordial de la vida de las personas dentro de sus trabajos, estudios, vida familiar y social.

Los delitos informáticos, son aquellos delitos que lesionan varios bienes jurídicos protegidos o varias conductas, -como es conocido actualmente-, por lo tanto se pueden considerar como pluriconductistas, algunos de estos son: propiedad, patrimonio, intimidad y adicionalmente causan daños.

Actualmente los delitos informáticos son considerados como "crímenes organizados transnacionales"1, debido al grado de criminalidad que pueden llegar a generar dentro de la sociedad.

Resulta más complicado en la actualidad el proceso de la averiguación del autor del delito informático y la reconstrucción de los elementos de convicción, es decir la prueba de los hechos,

1 Acurio, Santiago, "Derecho y Nuevas Tendencias", Corporación de Estudios y Publicaciones, Quito – Ecuador, 2010, Pág. 162.

esto se produce por la suficiencia del sistema jurídico, y específicamente en el Derecho Penal, no basta la presunción, si no es necesario que un hecho se reviste con el carácter de delito.

La deficiencia en la actualidad de los delitos informáticos se debe a que el Código Penal Ecuatoriano es de 1938, es decir que tiene aproximadamente setenta años de antigüedad, y por consiguiente la falta de tipificación de estos tipos de delitos, que son considerados noveles dentro de la sociedad no están tipificados con la respectiva prolijidad requerida de acuerdo al daño causado a las víctimas.

Existen dos causas que generan que esta clase de conductas delictivas permanezcan en la impunidad, debido a la falta de tipificación de los mismos, y estas son:

1.- Falta de conocimiento por parte de los encargados de la generar justicia.

2.- Falta de preparación de los organismos de administración de justicia y los cuerpos policiales, los cuales no poseen las herramientas adecuadas, ni necesarias para la investigar requerida para este tipo de delitos.2

Adicional a estas dos conductas que contribuyen a que el sujeto activo permanezca impune, existe otra característica que es el ANONIMATO de quienes generan este tipo de delitos dentro y fuera de sus países, y esto se produce debido a que quien comete el delito es una persona con un perfil criminológico propio, es decir diferente al de otros delincuentes que les permite sentirse y ser un tipo delincuencial que debe ser tratado y sancionado de acuerdo al daño que causaron.

Los delitos presentan cuatro categorías dogmáticas, que se convierten en base de conceptualización y de su posterior análisis correspondiente y estas son:

1.- Acto.

2 CFR, Acurio, Santiago, ¨Derecho y Nuevas Tecnologías¨, Corporaciones de Estudios y Publicaciones, Quito – Ecuador, 2010, Pág. 163.

2.- Tipicidad.

3.- Antijuricidad.

4.- Culpabilidad.

Dentro de estas, se presentaron con el transcurso del tiempo diferentes posturas, que han generado cambios dentro del estudio de los diferentes tipos de delitos, y estas son:

1.- Causalista:

a) Acto: Modificación del mundo exterior.

b) Tipicidad: Existe sujeto activo, sujeto pasivo, objeto material, conducta (bien jurídico protegido).

c) Antijuridicidad: Forma: acto y norma.

d) Culpabilidad: Dolo, culpa, imputabilidad.

2.- Neokantismo:

a) Acto: Modificación del mundo exterior.

b) Tipicidad: Elementos valorativos y descriptivos.

c) Antijuridicidad: Formal y material: daño real, verificable y confiable; puesta en peligro.

d) Culpabilidad: Dolo, culpa, imputabilidad.

3.- Finalismo – Post-finalismo.

a) Acto: Acción final.

b) Tipicidad: Objetiva: dolo y culpa; Subjetiva: Sujeto activo y sujeto pasivo, cosa – persona sobre la que recae el daño, conducta, objeto material y jurídico.

c) Antijuricidad: Formal y material.

d) Culpabilidad: Imputabilidad, exigibilidad, conocimiento de lo antijurídico.3

Los delitos informáticos dentro de este análisis estarían enmarcados dentro del finalismo y post-finalismo debido a que el acto va encausado en el perjuicio causado en la acción final, por consiguiente el delito informático sea cual sea el tipo de delito informático busca que el daño causado perjudique a sus víctimas.

Para Julio Téllez Valdés, la conceptualización de los delitos informáticos se marca dentro de dos acepciones típica y atípica, y de acuerdo a esta expresa:

1.- ¨Las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin¨.

2.- ¨Actitudes ilícitas en que se tienen a las computadoras como instrumento o fin¨.4

Algo que también es importante determinar dentro de los diferentes tipos de delitos informáticos son los sujetos activos que encontramos, la diferencia radical dentro de los ellos y los demás tipos de sujetos activos de cualquier otro tipo de delito -es decir homicidio, robo, violación, etc.- se encuentra en que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas

3 Datos obtenidos de la reunión con el Doctor Nicolás Salas, el día 08 de abril de 2011.

4 Téllez Valdés, Julio, ¨Los Delitos Informáticos¨, Situación en México, Informática y derecho No. 9, 10 y 11, UNED, Centro Regional de Extremadura, Mérida, 1996. Pág. 174.

informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, si bien son hábiles en el uso de los sistemas informatizados, aun cuando, en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.

Con el transcurso del tiempo se ha podido comprobar que los autores de los delitos informáticos son muy diversos y lo que los diferencia entre sí es la naturaleza de los delitos cometidos.

Para esto se plantea el siguiente ejemplo: La actividad es muy diferente entre la persona que entra en un sistema informático sin intenciones delictivas y el empleado de una institución financiera que desvía fondos de las cuentas de sus clientes.5
Específicamente hablando entre un hacker y cracker las diferencia entre ellos se específica en: las *técnicas* utilizadas para la realizar el ilícito; *sociales* debido a medio social dentro del cual se desenvuelve cada uno; económicas por beneficio propio; laborales por el tipo de trabajo que desempeñe cada uno.[6]

Otra de las características propias de los delitos informáticos es el ***dolo,*** si no existe este, no existe delito informático bajo ninguna perspectiva. Los delitos informáticos constituyen el dolo natural, esto es que existen dos características propias, que son:

1.- Conocimiento.

2.- Voluntad: querer hacer daño y conocer del daño que se va a causar.7

Uno de los temas que más importancia tiene dentro del estudio de los delitos informáticos es el *bien jurídico protegido*, para esto resulta primordial conceptualizar al mismo y es:

---

5 Acurio, Santiago, ¨Derecho y Nuevas Tecnologías¨, Corporaciones de Estudios y Publicaciones, Quito – Ecuador, 2010, Pág. 185.

[6] Cfr. Acurio, Santiago, ¨Derecho y Nuevas Tecnologías¨, Corporaciones de Estudios y Publicaciones, Quito – Ecuador, 2010, Pág. 193, 194, 195.

7 Datos obtenidos de la reunión con el Doctor Nicolás Salas, el día 08 de abril de 2011.

¨El bien que se lesiona por parte del o los sujetos activos, dentro del ilícito, y el mismo que se encuentra precautelado en la sociedad por las leyes y códigos¨.8

Los delitos informáticos presentan las características de lesionar varios bienes debido a que el daño causado puede ir direccionado a varios de estos, y algunos son:

1.- Patrimonio: en el caso de la amplia gama de fraudes informáticos y las manipulaciones de datos que da a lugar.

2.- Intimidad, reserva y confidencialidad: en el caso de las agresiones informáticas a la esfera de la intimidad e forma general, especialmente en el caso de los bancos de datos.

3.- Seguridad o fiabilidad del tráfico jurídico o probatorio: en el caso de falsificaciones de datos o documentos probatorios vía medios informáticos.

4.- Derecho de la propiedad: en este caso sobre la información o sobre los elementos físicos, materiales de un sistema informático, que es afectado por los de daños y el llamado terrorismo informático.

Por tanto, el bien jurídico protegido, acoge a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde ésta se almacena o transfiere.9

Dentro del presente trabajo se realizará un estudio e investigación de los siguientes tipos de delitos informáticos:

1.- Hacker.

2.- Cracker.

8 Notas Personales.

9 Acurio, Santiago, ¨Derecho y Nuevas Tecnologías¨, Corporaciones de Estudios y Publicaciones, Quito – Ecuador, 2010, Pág. 211.

3.- Phishing.

4.- Fraude Informático.

Cada sujeto activo dentro de estos tipos de delitos informáticos tiene una motivación que conlleva al cometimiento del delito, dentro de estas podemos encontrar a los siguientes:

1.- Motivación personal.

2.- Motivación económica

.

3.- Motivación psicológica

.

4.- Motivación social.

De estas circunstancias o motivaciones buscamos que cada sujeto activo busca una realización diferente, y por lo tanto no se puede sancionar a todos dentro de un mismo análisis o una misma tipificación, porque estaríamos cometiendo el error que actualmente existe en nuestro Código Penal.

Dentro del presente trabajo se encontrara que cada uno cada un tipo de delito que debe encuadrar dentro del Código penal de acuerdo a la magnitud del daño que puedan llegar a generar a cada persona y a la sociedad.

Estos tipos delitos informáticos tienen sus características propias y dentro de estos específicamente los tres primeros serán la base o el inicio para el cometimiento de otro tipo de delitos informáticos, es decir por lo tanto que generaran un doble daño a los diferentes bienes jurídicos protegidos que existen.

El principal problema para la permanencia impune de los sujetos activos de estos delitos, se produce debido a que en el Ecuador no existe una normativa que permita sancionar a los culpables de acuerdo a la magnitud del daño que puedan llegar a causar a la sociedad.

En los varios países del mundo ya se encuentra delimitado a este tipo de delitos, con lo cual ya existen varios individuos que ya han sido sancionados por el daño que causan, no solo a una persona en específico, sino también a entidades bancarias, gobiernos nacionales, entidades públicas y privadas, entre otras.

En el Ecuador cabe señalar, no es que no se encuentren delimitados los delitos informáticos, existe una tipificación dentro del Código Penal que configura varias figuras penales que encuadran con el perfil del sujeto activo de algunos tipos de delitos informáticos, pero el problema que se nos plantea en la actualidad es que no se encuadran, ni se tipifica a cada uno de ellos, que como sabemos poseen características diferentes y llegan a constituir cada uno un daño diferente e individualizado.

Además existen varios convenios internacionales que permiten sancionar a individuos que causan daño en otros países, dentro de esto tenemos específicamente ¨La Convención del Cybercrimen¨, la cual fue firmada por la Unión Europea en el año 2000, dentro de la misma existen conceptos, y además se permite la captura del delincuente informático dentro de los estados que hayan suscrito el convenio.

El Ecuador debe modificar sus leyes y códigos con el objetivo de que se regule y sancione a los culpables de los delitos informáticos, de acuerdo a la magnitud del daño que pueden llegar a causar a la sociedad, misma que se encuentra desprotegida en el tema, ya que como se ha citado el Ecuador no promulga un sistema jurídico en materia de delitos informáticos, lo que nos convierte en presa fácil de hackers, crackers, phishing y sobre todo de fraude informático, dado nuestro poco conocimiento.

Actualmente se considera como una prioridad notoria dentro de las instituciones públicas y privadas, y especialmente de las entidades bancarias una nueva regulación penal, que logre

sancionar a los respectivos culpables de los delitos informáticos y que adicionalmente se retribuya el daño causado a las víctimas de acuerdo a su grado de victimización.

Dentro de este trabajo se implanta nuevas tendencias de tipificar a cada uno de los delitos informáticos de acuerdo al daño que causan dentro de la sociedad ecuatoriana, como es sabotaje informático que incluso puede llegar a constituir como un tipo de terrorismo a nivel internacional, al phishing que genera constantes perjuicios a las entidades bancarias y a las personas naturales; por lo tanto se busca generar una nueva tendencia que contribuya de manera real a tipificar a los delitos informáticos.

Es por eso que la verdadera solución también está en una personalización por parte del Estado a través de su función legislativa, para que se planteen reformas y sobre todo una correcta difusión de los posibles problemas que pueden generar este tipo de sujetos cibernéticos.

Ya que solo una verdadera prevención evitara ser parte de un problema mundial, que tiene en zozobra a la mayoría de los países por no poder contrarrestar los peligrosos ataques.

La Constitución de la República del Ecuador, actual del año 2008, en su Título II Derechos, Capitulo Segundo Derechos del Buen Vivir, Sección Tercera Comunicación e Información, en su artículo 16, numeral 2 expresa:

> "Todas las personas, en forma individual o colectiva, tienen derecho a:
>
> … 2. El acceso universal a las tecnologías de información y comunicación…"

Esto es que a las personas dentro del territorio ecuatoriano se les garantiza el acceso y libre e independiente a la comunicación y por consiguiente a la tecnología, pero de la misma manera regula el derecho de la inviolabilidad de la intimidad, que dentro de mis análisis personales es el bien jurídico protegido que es violado por el sujeto activo que comete cualquier tipo de delito informático.

El marco de limitación del acceso libre a la tecnología, se encuentra dentro de la misma Constitución actual él su artículo 66, numeral 21, en el cual se expresa la inviolabilidad de la correspondencia tanto física como virtual, es decir limita el acceso a que cada persona tenga libre acceso a lo que realmente le pertenece y sea su propiedad.

Con el desarrollo de este trabajo se buscara analizar los principales problemas de tipificación y buscar una nueva tipificación nueva y generadora de un avance notable en el sistema judicial.

INDICE

INTRODUCCIÓN

La creación de la computación y posteriormente del Internet generaron una problemática: la aparición de individuos que por su estudio técnico o debido a su gran "inteligencia" logran acceder a la información de otras personas o de sus respectivos trabajos, labores o actividades.

Un hacker se define como, "un usuario de computadoras entusiasta y calificado, cuyo principal interés consiste en obtener un completo dominio de un sistema de computación y, mediante artilugios de programación, llevarlo a sus máximos niveles de rendimiento. En la actualidad, el término ha pasado a referirse a la persona que consigue acceso no autorizado a un sistema de computación y obtiene algún dominio sobre sus aplicaciones."[10]

Los hackers se consideran como "fanáticos de la informática, que son capaces con un modem, de acceder a redes de trasmisión de datos saltándose las medidas de seguridad".[11]

---

[10] Fuente Raúl Horacio Saroka, "Sistemas de Información", Fundación OSDE, 1998, Pág. 55

[11] Orlando Solano; "Trascripción de su obra Manual de la Informática"; Concepto de Hacker; Pág. 288.

Los conceptos expuestos, nos permiten determinar que un “hacker” es aquella persona con conocimientos extensos de Informática e Internet, adquiridos sea por medio de estudios o por investigaciones personales continuas, que los lleva a conocer a profundidad el campo informático.

Una de las definiciones que considero transcendental dentro de este análisis, es el relacionado a los delitos informáticos:

“El delito informático implica actividades criminales, que con la ayuda de la informática o de técnicas anexas, que llegan a configurarse como robos, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, entre otros.”[12]

Los delitos informáticos como queda consignado, son actividades que generan un gran perjuicio a las personas que los sufren, sea cual sea la forma en que se los ejecute. La información que contiene cada persona en la índole que sea, es decir, datos, cifras, informes, información laboral, información personal, entre otras debe ser exclusivamente de uso personal, como lo consagra la Constitución de la República.

> “El derecho a la protección de datos de carácter personal…” [13]

[12] Sandra Jeannette Castro Ospina, “Universidad Externado de Colombia”, ponencia presentada dentro de las XXIII Jornadas Internacionales de Derecho Penal, Colombia, "Delitos Informáticos", 15 de Julio 2002, en http://www.delitosinformaticos.com/delitos/colombia.shtml.

[13] Constitución de la República del Ecuador, Artículo 66, numeral 19.

La norma constitucional referida, garantiza la privacidad de la información personal de los ciudadanos, disposición que se refleja en la Legislación Nacional, que más adelante expondremos.

¿Cómo establecer la culpabilidad del hacker, cracker, phishing y de quién realiza fraude informático?, sería la pregunta que deberíamos plantearnos, debido a que la legislación nacional y el proceso penal se basan en una búsqueda de elementos de convicción mediante la investigación del delito cometido, para sancionar al culpable del mismo.

En nuestra Legislación, no se ha diferenciado a los hackers de los crackers, o a los crackers de los phishing y a quien comete fraude informático, solamente se sanciona a quien accede a la información ajena, pero es trascendental realizar una clara diferencia.

El objetivo principal de plantear diferencias radica en establecer el tipo de sanción que pueden imponerse a los partícipes de esta gama de delitos, toda vez que teniendo una clara tipología criminal, podremos aplicar las penas de acuerdo a la gravedad y daño del hecho por una parte y por otra, podrían aplicarse medidas alternativas, por ejemplo en el caso del hacker, cuyos conocimientos sobre Informática pueden resultar beneficiosos para la sociedad.

En el análisis de las tipologías en los delitos informáticos pretenderemos demostrar que es necesario y fundamental un cambio, debido a que la tecnología avanza a pasos agigantados cada día.

Pretenderemos además realizar un análisis con legislaciones internacionales, las cuales servirán de apoyo para lograr un proyecto nuevo y mejorado; que nos permita incriminar y sancionar las conductas que devienen de esta área, a fin de precautelar tanto la seguridad ciudadana, como el derecho a la privacidad, bien jurídico tutelado por el Estado, que se ve lesionado con este tipo de delitos.

CAPÍTULO I: CONCEPTOS Y DEFINICIONES

1.1. DEFINICIÓN DE DELITOS INFORMÁTICOS

Tanto la Legislación Nacional como la Internacional, evidencian dificultades al momento de conceptualizar a los Delitos Informáticos, ya que deben ser considerados en el catálogo de figuras típicas, tomando en cuenta la continua evolución que por su naturaleza poseen. La Legislación más avanzada en temas informáticos es la española, que presenta conceptualizaciones que le han permitido tipificar este tipo de conductas, de acuerdo a los avances tecnológicos, que incluyen los hackers, crackers, phishing y los delitos informáticos.

Para definir que es un delito informático, resulta transcendental especificar que es delito, y después establecer que es informática, para luego conceptualizar qué es del delito informático. "El delito etimológicamente proviene del latín delictum, expresión también de un hecho antijurídico y doloso castigado con una pena."[14]

[14] CABANELLAS, Guillermo; "Diccionario Jurídico Elemental; Edición 16; Año 2003; Editorial Heliasta; Pág.: 115.

“El delito como acto típicamente antijurídico imputable y culpable, sometido a veces a condiciones objetivas de penalidad y que se halla conminado con una pena o, en ciertos casos, con determinada medida de seguridad en reemplazo de ella.”[15]

El delito según la conceptualización conocida dentro de la Legislación Nacional es el acto típico, antijurídico, culpable y punible. La sanción será el resultado de la tipificación del delito cometido. La palabra informática en cambio Proviene del francés informatique, implementado por el ingeniero Philippe Dreyfus a comienzos de la década de los 60’. Informática a su vez está formada del conjunto de palabras como son information *y* automatique (información y automática*).* Por lo tanto podemos decir que la definición de informática:

“Es el procesamiento automático de información mediante dispositivos electrónicos y sistemas computacionales”[16]

El término “información”, que según la definición de la Real Academia de la Lengua Española significa: “enterar, dar noticia de algo” y que en términos legos hubiera significado tan sólo una simple acumulación de datos, se ha ampliado, transformándose como advierte Gutiérrez Francés: "en un valor, un interés social valioso, con frecuencia cualitativamente distinto, dotado de autonomía y objeto del tráfico."[17]

[15] Concepto de Jiménez de Azua, dentro de la obra de Dr. Vicente Vallejo, “El Delito Informático en la Legislación Ecuatoriana”, Corporación de Estudios y Publicaciones, 2010, Quito-Ecuador, Pág. 11.

[16]Diccionario de Informática, actualizada a marzo 15 de 2011, Autores Avisos Google, http://definicion.de/informatica/

[17] Gutiérrez Francés, Mariluz. Notas sobre la delincuencia informática: atentados contra la "información" como valor económico de empresa, en: Mazuelos Coello, Julio (comp.). Derecho Penal Económico y de la Empresa, pág. 383, primera edición, Edit. San Marcos, Lima, 1997.

Una vez que los conceptos de delito e informática, han quedado consignados, cabe definir al delito informático expresando que 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."[18]

"También entendiéndoles como todo acto intencional asociado de una manera u otra a los computadores; en los cuales la victima ha o habría podido sufrir una perdida; y cuyo autor ha o habría podido obtener un beneficio."[19]

Es necesario resaltarlo, pues se suele confundir al Derecho de la informática con la informática jurídica, que no es sino aplicar los sistemas informáticos a la resolución de problemas específicos de los profesionales del Derecho, como puede ser la búsqueda de información documental o la tramitación de asuntos, por ejemplo. La informática jurídica es la tecnología que se ocupa del problema jurídico, sea a través de la creación de bases de datos jurídicos, de programas para la gestión propia de los profesionales del Derecho, o incluso, a través de sistemas informáticos que apoyan la toma de decisiones jurídicas. No es derecho informático, no es norma jurídica, no es derecho.

"Delito informático, crimen genérico o crimen electrónico, que agobia con operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores, medios electrónicos y redes de Internet."[20]

[18] CFR, María José Viega; "Un Nuevo Desafío Jurídico: Delitos Informáticos"; Ed. Mc Graw – Hiu, México, 1996, Pág. 26.

[19] Parker, D.B., Citado por ROMERO CASABONA, Carlos M., "Poder Informático y Seguridad Jurídica", Madrid – España, 1987, dentro de la Obra "Derecho y Nuevas Tecnologías", Santiago Acurio, Corporación de Estudios y Publicaciones, Quito – Ecuador, 2010, Pág. 175.

[20] "Delito Informático", Enciclopedia Libre Wikipedía, actualizada a 25 de febrero de 2011, http://es.wikipedia.org/wiki/Delito_inform%C3%A1tico

Delito informático es aquél en que el uso de un computador o el acceso al mismo o a sus partes componentes (terminales, redes, bases de datos, etc.) es un elemento esencial, de modo tal que el delito no podría haberse cometido sin aquel uso o acceso.[21]

Como vemos, los delitos informáticos son actividades que causan y generan un gran perjuicio a las personas que los sufren. El primer problema que se generó en la informática dentro de la era del Internet fueron los virus, aquellos que ingresaban al sistema y dañaban el mismo y a toda la información que tenía el propietario, y la solución que se encuentra a este daño es eliminar toda la información que existe en el sistema informático.

Ante este primer tipo de problemas jurídicos, se manifestaron principios de seguridad informática, los cuales buscaban regular las irregularidades existentes y que a futuro se generarían, estos son:

1. El intruso al sistema utilizará cualquier artilugio que haga más fácil su acceso y posterior ataque. Existirá una diversidad de frentes desde los que puede producirse un ataque. Esto dificulta el análisis de riesgos porque el delincuente aplica la filosofía del punto más débil de este principio.

2. Los datos deben protegerse solo hasta que pierdan su valor. Se habla, por tanto, de la caducidad del sistema de protección: el tiempo en el que debe mantenerse la confidencialidad o secreto del dato.

[21] CFR, Dr. Vicente Vallejo, "Delito Informática en la Legislación Ecuatoriana", Corporación de Estudios y Publicaciones, 2010, Quito-Ecuador, Pág. 12.

3. Las medidas de control se implementan para ser utilizadas de forma efectiva. Deben ser eficientes, fáciles de usar y apropiadas al medio. Ningún sistema de control resulta efectivo hasta que es utilizado al surgir la necesidad de aplicarlo.

1.2. DEFINICIÓN DE HACKER Y CRACKER

Como un hacker podemos considerar a:

> "Pirata informático, intruso informático." [22]

Por lo tanto el hacker es una persona que actúa robando información de otras personas, ingresando a los códigos informáticos privados. El objetivo del hacker es utilizar esa información con el fin de realizar actos ilícitos a favor propio y en contra de aquel a quien robo la información.

Además se considera al hacker como:

"Un programador que escribe programas en lenguaje ensamblador o en lenguaje a nivel de sistemas, como C. Si bien esto puede referirse a cualquier programador, implica un muy tedioso <<desmenuzamiento>> de bits y bytes. Algunas veces se refiere a una persona que viola un código y obtiene ingreso ilegal a un sistema".[23]

[22] Diccionario de Computación Bilingüe; FREEDMAN, Alan; Tomo 2; Concepto de Hacker, Página: 337.

[23] Ibídem.

"De acuerdo con la acepción original del término, un "hacker" es un usuario de computadoras entusiasta y calificado, cuyo principal interés consiste en obtener un completo dominio de un sistema de computación y, mediante artilugios de programación, llevarlo a sus máximos niveles de rendimiento. En la actualidad, el término ha pasado a referirse a la persona que consigue acceso no autorizado a un sistema de computación y obtiene algún dominio sobre sus aplicaciones."[24]

El Hacker, en el contexto actual del término, es una persona que con conocimientos técnicos o especializados, busca acceder a la información de otra persona o de una institución, con el fin de conocer esta información. La diferencia principal entre un "Hacker" y "Cracker", es que el primero es un usuario en computación cuya intención es buscar el dominio del sistema informático, mientras que el segundo es aquel que ingresa al sistema violando la seguridad informática.

El principal problema que existe en nuestra Legislación es la confusión que existe entre estos dos términos, debido a que los Delitos Informáticos todavía tienen grandes deficiencias dentro de la tipificación actual. En ningún concepto se establece al Hacker como un criminal, y ese también es uno de los problemas con los que nos encontramos, ya que se lo considera una persona "inteligente y no criminal", por lo mismo el hecho de conceptualizar sus actos como delitos se convierte en algo difícil y complejo.

Es por eso que el presente trabajo tiene como objetivo, demostrar las conductas que diferencian al hacker criminal, que en este caso se denominará CRACKER que una especie de hacker de cuyas conductas se derivan actos delictivos. El problema principal como lo he referido en líneas anteriores, radica en que resulta altamente complicado determinar qué conductas corresponden a actos correctos o lesivos, y esto es lo que hace peligroso y complicado diferenciarlo de entre las demás personas, pues el hacker tiene la habilidad de mezclarse con las personas comunes, sin

[24] Fuente: Raúl Horacio Saroka, "Sistemas de Información", Fundación OSDE, 1998, Pág. 67.

poder distinguirlo hasta que no empieza a utilizar procedimientos que revelan su capacidad tecnológica.

Por lo tanto, una de las características principales de los hackers, es su inteligencia, son individuos con una inteligencia superior, lo cual les hace diferenciar del común de las personas y les permite realizar sus actos sean lícitos e ilícitos. Los hackers además tienen dos características primordiales realizan sus actos individuales, nunca los realizan con alguien más, y son totalmente anticonformistas, buscan la perfección a costa de lo que sea. En base a estas características se puede establecer que el hacker es una persona "especial", con capacidades intelectuales que los convierten en dos tipos de personas: criminales o personas capaces de contribuir en temas informáticos.

Otro concepto obtenido del hacker es: "Término para designar a alguien con talento, conocimiento, inteligencia e ingenuidad, especialmente relacionadas con las operaciones de computadora, redes, seguridad, etc."[25]

Por lo tanto el hacker es todo aquel individuo con conocimientos suficientes en informática y con capacidad intelectual sumamente alta, que puede llegar a obtener beneficios sean lícitos o ilícitos de sus actos.

Definiendo al cracker podemos decir: "Experto que entra en los sistemas informáticos de forma furtiva y con malas intenciones. Suele contar con tecnologías avanzadas para cometer sus acciones y es capaz de deteriorar complejos sistemas."[26]

[25] "Concepto de Hacker", Enciclopedia Seguridada.Net, actualizada a 28 de marzo de 2011, http://www.seguridadpc.net/hackers.htm

[26] "Definición de Cracker", Enciclopedia Proyecto de Fin de Carrera, actualizado a 25 de marzo de 2011, http://www.proyectosfindecarrera.com/definicion/cracker.htm

Persona que viola la seguridad de un sistema informático con fines de beneficio personal o para hacer daño. A su vez diseña o programa cracks informáticos, que sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican.

"Persona que practica el cracking, acción de modificar el código fuente a un programa."[27]

El cracker a diferencia del hacker es una persona que solamente busca hacer daño con sus actos, accede a la información de otra persona o a la información de una entidad pública o privada buscando lesionarla no tiene una finalidad lícita. Los crackers son personas sin una inteligencia o una capacidad intelectual superior, estos simplemente acceden a la información como un fanatismo o como un juego que los lleva a obtener beneficios ilícitos.

El término cracker viene del inglés crack, que significa romper. Un cracker es alguien que viola la seguridad de un sistema informático de forma similar a como lo haría un hacker, sólo que a diferencia de este último, el cracker realiza la intrusión con fines de beneficio personal o para hacer daño. El término cracker se deriva de la expresión "criminal hacker", y fue creado alrededor de 1985 por contraposición al término hacker, en defensa de éstos últimos por el uso incorrecto del término. Se considera que la actividad de esta clase de cracker es dañina e ilegal.

También se denomina cracker a quien diseña o programa cracks informáticos, que sirven para modificar el comportamiento o ampliar la funcionalidad del software o hardware original al que se aplican, sin que en absoluto pretenda ser dañino para el usuario del mismo. No puede considerarse que la actividad de esta clase de cracker sea ilegal si ha obtenido el software o hardware legítimamente, aunque la distribución de los cracks pudiera serlo. Asimismo, un cracker también es aquel que practica el cracking (acción de modificar el código fuente a un

[27] "Definición de Cracker", Glosario Pergamino Virtual, actualizado al año 2009, http://www.pergaminovirtual.com/definicion/Cracker.html?PHPSESSID=6ca66c36adfd500ec95c3aa18b82e9d6

programa). Ésta actividad está prohibida a menos que el programa al que se le aplica sea de Software libre, y por lo general requiere muchos conocimientos sobre hacking.

En pocas palabras el cracker se dedica a romper candados y obtener números de serie para los programas comerciales; roba información y se dedica a corromper los sistemas que desee. A diferencia de los hackers que, si bien, también se dedican a encontrar las vulnerabilidades en los sistemas para explotarlos; los crackers no proporcionan una solución a dichos fallos como bien lo hacen los hackers.

1.3. DEFINICIÓN DE PHISHING

Después de haber aclarado las definiciones de hacker y cracker, ahora analizaré un nuevo concepto que no es muy conocido dentro de la Legislación Nacional, pero sí en la Legislación Internacional, en la que su conducta se encuentra tipificada de acuerdo al daño que pueden causar.

"Consiste en el envío de correos electrónicos que, aparentando provenir de fuentes fiables (por ejemplo, entidades bancarias), intentan obtener datos confidenciales del usuario. Para ello, suelen incluir un enlace que, al ser pulsado, lleva a páginas web falsificadas." [28]

De esta manera, el usuario, creyendo estar en un sitio de toda confianza, introduce la información solicitada que, en realidad, va a parar a manos delincuenciales. Es por eso que existe un amplio abanico de software y aplicaciones de toda índole que quedan clasificados dentro de la categoría de robo de información personal o financiera, algunas de ellas realmente complejas, como el uso

[28] "Definición de Phishing", Enciclopedia Seguridada.Net, actualizada a 28 de marzo de 2011, http://www.seguridadpc.net/phishing.htm

de una ventana Javascript flotante sobre la barra de direcciones del navegador con el fin de confundir al usuario.

Por lo tanto el phishing es un fraude de tipo cibernético. Consiste en el envío de un e-mail a millones de personas con la finalidad de “robarle” información “delicada” como: claves de tarjetas, passwords de bancos, contraseñas de páginas web, etc. Simula ser enviado por alguna institución seria y reconocida, imitando su logotipo y sus colores y se le pide al receptor que haga click en algún link que, en realidad lo conduce a una página pirata (aunque tenga la apariencia de ser original y legal). Aparecerá una pantalla, que con algún pretexto le pedirá introducir claves secretas o números de identificación de alguna cuenta. Si el usuario no se percata del timo, estará suministrando a los delincuentes su información confidencial y sus cuentas se verán afectadas.

Algunos de los riesgos del phishing y de otorgar la información a otra persona son:

1. Los datos facilitados pueden ser empleados por el pirata para acceder a las cuentas de los usuarios y gestionar su dinero o realizar compras sin su autorización o consentimiento.

2. Puede emplearlos para abrir nuevas cuentas bancarias o tarjetas de créditos en nombre de la "víctima" pero con otra dirección física de correo, lo que supone un robo de identidad.

3. El equipo de la víctima puede servir para difundir virus programados para hacer llegar los e-mails fraudulentos a más usuarios.

Se recomienda a los usuarios que revisen la legalidad y veracidad de todos los emails que reciban con cualquier tipo de información y más aun de aquellas en las cuales se solicite algún tipo de información privada.

1.4. FRAUDE INFORMÁTICO

El fraude es más conocido en la Legislación Nacional, pero también es importante conocer el concepto especifico de las palabras y a su vez establecer un concepto integral del término.

- Fraude: es todo abuso de confianza.

- Informática: todo aquello relacionado con la computación, sistemas, electrónica y el Internet.

Por lo tanto el concepto de Fraude Informático: Es el engaño, abuso de confianza, astucia, o maquinación de que uno se sirve, hablando u obrando con mentira o artificio para obtener información informática de las personas o entidades públicas o privadas. Es importante entender que no hay fraude informático, sin un engaño previo, por eso es importante aclarar que este se realizará por personas conocidas que se aprovechan de la confianza en ellas depositada a fin de acceder al engaño o fraude. El engaño aparece en la conducta de quien procede con dolo y el fraude no es sino el perjuicio proveniente de haber sido engañado.

1.5. ANÁLISIS GENERAL DEL TEMA

Los delitos informáticos, y sus formas de delinquir son en gran medida desconocidos para la población común, así como sus definiciones, posibles tipificaciones, alcance de daño y las sanciones que pueden llegar a contemplar. Uno de los problemas que puede llegar a plantearse es que una vez conocidas las definiciones, se desconozca cual es la magnitud de la gravedad del daño que causan y como puede encontrarse la solución a los mismos, como se configura al sujeto pasivo, sujeto activo y al bien jurídico protegido que se esté violando en la realización del delito informático.

Lo principal para establecer las diferencias entre las conductas delictivas, es conocer las definiciones de las mismas, para identificar cuando el daño lo realiza un cracker, o un hacker, cuando se trata de un email con contenido phishing o cuando se trata de un fraude informático y poder hacer la respectiva denuncia a las autoridades para que el culpable cumpla con la sanción respectiva y repare a la víctima. Resulta imprescindible que se incorpore a la legislación nacional, la adecuación típica y antijurídica, a fin de incriminar estos nuevos tipos de delitos y de esta forma, adaptar nuestra normativa a esta nueva forma criminal, que en los últimos años, ha incrementado su injerencia en el país.

CAPÍTULO II: HACKER EN LA LEY PENAL

2.1. TRATAMIENTO JURÍDICO

Una vez aclarado el concepto de hacker, es importante ahora analizar cuál es el tratamiento legal que le otorga la Ley a los hackers en el Ecuador. Como lo señalamos, al hacker se lo debe diferenciar de acuerdo a la forma conductual, porque estos pueden ser beneficiosos para la comunidad o dañinos para la sociedad, en cuyo caso, se requiere tipificar la conducta y establecer sus sanciones, como ocurre en otras legislaciones. El tratamiento jurídico que daré al hacker será bajo el análisis de la estructura del delito, el análisis de la tipificación objetiva y bajo los principios jurídicos que rigen al proceso penal.

Tratadistas Españoles, - debido a que España es uno de los países más desarrollados en temas informáticos y por lo tanto se convierte en un modelo a seguir para los demás países del mundo,- han considerado que para realizar el tratamiento jurídico de los hackers, es necesario conocer los siguientes puntos, dentro de la tipificación:

Análisis Jurídico:

Dentro de la tipificación se puede realizar el siguiente análisis, que puede convertirse en la base para la posibilidad de la identificación del dolo y culpa del posible sujeto activo de un delito.

1. Sujeto activo: Fanático de la informática que ingresa al sistema informático con voluntad y conciencia con la finalidad de causar daño – Hacker.

2. Sujeto pasivo: Persona que es víctima del delito cometido – Cualquier persona – entidad pública o privada.

3. Verbo rector: Es la base con la cual se tipifica al delito y al daño que causan. – violación a la privacidad.

4. Bien jurídico protegido: También conocida como conducta "Su esencia consiste en la relación de disponibilidad de un sujeto con un objeto."[29] – Información personal – privacidad.

De esta manera identificamos los elementos del delito informático, para poder tipificarlo de acuerdo al perfil del tratamiento jurídico dado.

[29] ZAFFARONI, Eugenio Raúl; "Manual de Derecho Penal"; Parte General; Primera Edición; Buenos Aires, Argentina; 2005, Página 369.

2.1.1 Estructura del Delito Informático - Hacker

1. Por la gravedad: "Son infracciones los actos imputables sancionados por las leyes penales, y se dividen en delitos y contravenciones, según la naturaleza de la pena peculiar."[30]

   Por lo tanto, la conducta ilícita que desarrollan los hackers puede catalogarse como delictiva, al actuar dolosamente y provocar grandes perjuicios a los sujetos pasivos de la infracción, el mismo que establecerá una pena y multa.

2. Por su estructura***:*** Complejos, porque su daño lesiona a más de un bien jurídico. En el delito cometido por los hackers encontramos que los siguientes bienes jurídicos lesionados:

   1. a.- Violación de la privacidad.
   2. b.- Violación del derecho a la intimidad.
   3. c.- Violación de la información personal.

3. Por la duración: Pueden ser instantáneos, permanentes o continuados. Permanentes, porque su consumación puede durar un lapso de tiempo largo, según el daño causado al sistema protegido (información, software, hardware), tanto más que la intervención de los hackers, producen daños a la información y sus efectos pueden extenderse en el tiempo.

[30] Código Penal; Título II De las Infracciones en General; Capítulo I De la Infracción Consumida y de la Tentativa; Artículo 10.- Infracciones.

4. Por sus efectos: Daño, por la afectación del bien jurídico tutelado. El efecto que causa la conducta delictiva de los hackers es el daño, y la afectación al bien jurídico protegido. No son los hackers como figura, el delito penal que debe ser tipificado, sino la conducta delictiva que estos pueden desarrollar y legar a cometer actos que constituyen un delito y por lo tanto merecen ser investigados, para poder aplicar la sanción correspondiente.

2.1.2 Principios del Proceso Penal

Los principios del proceso son las garantías que protegen a las partes que intervienen en dentro del mismo. Los principios y garantías constitucionales, son la base de la legalidad del proceso penal, de la igualdad de las partes procesales y de una correcta administración de justicia.

1. Principio de Legalidad: "Nadie puede ser juzgado ni sancionado por un acto u omisión que, al momento de cometerse, no este tipificado en la ley como infracción penal, administrativa o de otra naturaleza; ni se le aplicará una sanción no prevista por la Constitución o la ley. Sólo se podrá juzgar a una persona ante un juez o autoridad competente y con observancia del trámite propio para cada procedimiento."[31]

Principio en base al cual, la persecución penal del delito, requiere una tipificación y sanción previas. La conducta delictiva dolosa, claramente diferenciada, será motivo de una tipificación penal, y la sanción posterior a las personas será la consecución de la misma.

[31] Constitución de la República del Ecuador; Titulo II Derechos; Capítulo Octavo; Derechos de Protección; Artículo 76; Numeral 3; Página 59.

2.2. Tipificación actual

Además de lo que se encuentra tipificado actualmente en el Código Penal, tenemos la norma constitucional que protege el derecho de libertad de la información personal. En el Código Penal se encuentran tipificados cierta cantidad de artículos, los cuales buscan regular el daño que causan quienes realizan algún delito informático. Dentro de la tipificación, el que considero que se encuentra en relación con la conducta delictiva realizada por el hacker, es el 202.1 del texto legal antes referido.

Que expresa lo siguiente:

- **"**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 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 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, estas

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."[32]

Análisis del Texto Legal

- Sujeto Activo.- Hacker – cracker.
- Sujeto Pasivo.- Cualquier persona – entidad pública o privada.
- Bien Jurídico Protegido.- Información pública o privada; derecho a la intimidad; información personal.
- Verbo rector 1.- Violentar claves o sistemas de seguridad, divulgar o utilizar fraudulentamente la información protegida.
- Finalidad: (Del acto delictivo)
    1. Acceder u obtener información protegida, contenida en sistemas de información.
    2. Vulnerar el secreto, confidencialidad y reserva, o simplemente la seguridad.
- Sujeto Activo - Agravante.- Personas encargadas de la custodia o utilización legitima de la información.
- Penas.- (De acuerdo a la gradación de menor a mayor).

[32] Código Penal; Título II De los Delitos contra las Garantías Constitucionales y la Igualdad Racial; Capítulo V; De los Delitos contra la Inviolabilidad de Domicilio; Artículo 202.1.- Delitos contra la Información Protegida; Página 40.

1. Prisión de seis meses a un año.
2. Prisión de uno a tres años.
3. Reclusión menor ordinaria de tres a seis años.

- Agravante.- Reclusión menor de seis a nueve años.

- Multas.-

1.- Quinientos a mil dólares de los Estados Unidos de Norteamérica.

2.- Mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

3.- Dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

- Agravante.- Dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Dentro de esta tipificación, la más afín a la conducta delictiva realizada por los hackers, no se diferencia el dolo**,** que se constituye en la diferencia entre los hackers buenos y malos, porque no debemos olvidar que esta diferenciación existe.

"El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual; ésta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención

judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motive su examen. Este derecho protege cualquier otro tipo o forma de comunicación."[33]

El problema principal dentro de esta tipificación en el Código Penal, es que ya quedo totalmente en el pasado, no se hace ninguna especificación de la conducta delictiva del sujeto activo que causa el daño, no se ha actualizado las penas, con penas alternativas que serían totalmente más beneficiosas que seguir llenando las cárceles, - que ya se encuentran abarrotadas - sin generar una rehabilitación social íntegra y sin lograr un reintegro a la sociedad, algo que hasta el momento no ocurre.

Dentro de este análisis se puede distinguir con claridad que aunque se encuentra tipificado a cierta parte del acto delictivo que pueden provocar los hackers que actúan con dolo, es decir con mala fe, no se diferencia a aquellos que lo realizan de buena fe, es decir sin la intención de causar daño a las personas.

2.3 Análisis de las posibles reformas al Código Penal

Es importante analizar ahora cuales serían los cambios que se tendría en el país, si se llega a modificar el Código actual.

[33] Constitución de la República del Ecuador; Titulo II; Capítulo Sexto; Derechos de Libertad; Artículo 66; Numeral 21; Página 55.

2.3.1 Reformas Dogmáticas

- Uno de los cambios que dogmáticamente encontraríamos en la nueva tipificación del Código Penal, es que el delito es considerado como una infracción penal que tiene cierta gravedad al punto de que podría ser sancionada con penas privativas de libertad de uno o varios años.

- Otro de los cambios que se podrían encontrar es que se van a introducir nuevas formas de tipificar daños graves a los derechos humanos, como los delitos informáticos y las infracciones al régimen de desarrollo.

- En la nueva tipificación encontraríamos a los delitos informáticos dentro del Libro I La Infracción Penal, Título II Los Delitos, Sección IV Delitos contra el Derecho a la Intimidad e Inviolabilidad del Domicilio; además Sección V Delitos contra el Derecho a la Propiedad.

2.3.2 Reformas Específicas

- Las nuevas propuestas que existen para mejorar al Código Penal actual y en específico sobre la tipificación que existe sobre los delitos informáticos son los siguientes.

2.3.2.1 Delitos contra el derecho a la intimidad e inviolabilidad de domicilio

2.3.2.1.1. Base ilegal de datos.-

Será sancionada hasta con seis (6) meses de restricción de libertad la persona que acceda, obtenga, compile, archive o procese datos de otra sin su autorización.

Análisis:

- Sujeto Activo.- Cualquier persona.
- Sujeto Pasivo.- Cualquier persona.
- Verbo Rector 1.- Acceder a los datos.
- Verbo Rector 2.- Obtener datos.
- Verbo Rector 3.- Compile datos.
- Verbo Rector 4.- Archive datos.
- Verbo Rector 5.- Procese datos.
- Pena.- Seis meses de restricción de libertad.

2.3.2.1.2. Violación de Privacidad.-

Será sancionada hasta con tres (3) meses de restricción de libertad la persona vulnere por cualquier medio la privacidad de otra. La pena será de hasta seis (6) meses si se publica o difunde por cualquier medio la información obtenida violando la privacidad.

Análisis:

- Sujeto Activo.- Cualquier persona.
- Sujeto Pasivo.- Cualquier persona.
- Verbo Rector.- Vulnerar la privacidad.
- Pena.- Tres meses de restricción de libertad.
- Agravante.- Publicar o difundir en cualquier medio la información.
- Pena Agravante.- Seis meses de restricción de libertad.

2.3.2.1.3 Violación de comunicación privada.-

Será sancionada hasta con tres (3) meses de restricción de libertad la persona que acceda, intervenga, retenga, revele o publique por distinto medio, sin autorización de su titular, cualquier tipo de comunicación privada no destinada a ella.

Análisis:

- Sujeto Activo.- Cualquier persona.
- Sujeto Pasivo.- Cualquier persona.

- Verbo Rector 1.- Acceder a comunicación privada.
- Verbo Rector 2.- Intervenir en comunicación privada.
- Verbo Rector 3.- Retener comunicación privada.
- Verbo Rector 4.- Revelar comunicación privada.
- Verbo Rector 5.- Publicar comunicación privada.
- Pena.- Tres meses de restricción de libertad.

2.3.2.2 Delitos contra el derecho a la propiedad

2.3.2.2.1 Distorsión de información relevante.-

Será sancionada con pena de restricción de libertad de hasta seis (6) meses la persona que, en perjuicio de otra que tiene derecho a su acceso, oculte o distorsione información económica o financiera sobre sí mismo o sobre la entidad o empresa que representa, dirija o administre.

Análisis:

- Sujeto Activo.- Cualquier persona.
- Sujeto Pasivo.- Cualquier persona.
- Verbo Rector 1.- Ocultar información económica o financiera sobre sí mismo o sobre la identidad que represente, dirija o administre.

- Verbo Rector 2.- Distorsionar información económica o financiera sobre sí mismo o sobre la identidad que represente, dirija o administre.

- Pena.- Seis meses de restricción de libertad.

2.3.2.2.2. Daño informático.-

Será sancionada con pena de hasta seis (6) meses de restricción de libertad la persona que destruya, impida o altere la utilización de datos o programas contenidos en soportes magnéticos, electrónicos o informáticos de cualquier tipo, o durante un proceso de transmisión de datos. La misma pena se aplicará a quien venda o distribuya de cualquier manera programas destinados a causar los efectos señalados anteriormente. La pena será de hasta un (1) año de restricción de libertad si el daño se produce sobre sistemas informáticos científicos, culturales, militares o cualquier otra que paralicen servicios públicos o privados.

Análisis:

- Sujeto Activo.- Cualquier persona.

- Sujeto Pasivo.- Cualquier persona.

- Verbo Rector 1.- Destruir la utilización de datos o programas contenidos en soportes magnéticos, electrónicos o informáticos de cualquier tipo o durante un proceso de transmisión de datos.

- Verbo Rector 2.- Impedir la utilización de datos o programas contenidos en soportes magnéticos, electrónicos o informáticos de cualquier tipo o durante un proceso de transmisión de datos.

- Verbo Rector 3.- Alterar la utilización de datos o programas contenidos en soportes magnéticos, electrónicos o informáticos de cualquier tipo o durante un proceso de transmisión de datos.

- Verbo Rector 4.- Vender la utilización de datos o programas contenidos en soportes magnéticos, electrónicos o informáticos de cualquier tipo o durante un proceso de transmisión de datos.

- Verbo Rector 5.- Distribuir la utilización de datos o programas contenidos en soportes magnéticos, electrónicos o informáticos de cualquier tipo o durante un proceso de transmisión de datos.

- Pena.- Seis meses de restricción de libertad.

- Agravante.- Un año de restricción de libertad, si se realiza a sistemas informáticos, culturales, militares que paralicen servicios públicos o privados.

2.3.2.2.3 Destrucción de instalaciones de transmisión de datos.-

Será sancionada con una pena de hasta un (1) año de restricción de libertad la persona que destruya la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos.

Análisis:

- Sujeto Activo.- Cualquier persona.

- Sujeto Pasivo.- Cualquier persona.

- Verbo Rector.- Destruir la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensaje de datos.

- Pena.- Un año de restricción de libertad.

2.3.2.2.4. Revelación de información confidencial o comercial.-

Será sancionada con pena de restricción de libertad de hasta tres (3) meses la persona que divulgue o utilice indebidamente información confidencial o secreta que haya obtenido en virtud de su vinculación con una persona natural o jurídica.

La pena será de hasta seis (6) meses de restricción de libertad si se devela secretos comerciales que pongan en riesgo su actividad comercial.

Análisis:

- Sujeto Activo.- Cualquier persona.
- Sujeto Pasivo.- Cualquier persona.
- Verbo Rector 1.- Divulgar indebidamente información confidencial o secreta que haya obtenido en virtud de su vinculación con una persona natural o jurídica.
- Verbo Rector 2.- Utilizar indebidamente información confidencial o secreta que haya obtenido en virtud de su vinculación con una persona natural o jurídica.
- Pena.- Tres meses de restricción de libertad.
- Agravante.- Seis meses de restricción de libertad si se devela secretos comerciales que pongan en riesgo su actividad comercial.

Análisis final:

Estas reformas generarían un avance notorio e importante dentro de la tipificación que existe en la ley penal. Lo que para mi parecer faltaría es establecer la conducta delictiva del sujeto activo -como ya lo he mencionado anteriormente- que permitiría sancionar al culpable de acuerdo al nivel de culpabilidad que genera sus actos, ya sea en el caso del hacker, cracker, phishing y en el de fraude informático.

2.4 POSIBILIDAD DE PENAS ALTERNATIVAS Y CASUÍSTICAS

Una vez analizado lo que se encuentra tipificado actualmente y las posibles reformas que podrían existir acerca de los delitos informáticos, ahora se procederá con la exposición del tipo de penas que se puede interponer a los hackers de acuerdo al daño que causaron a sus víctimas. No basta con señalar los conceptos y definiciones sobre los hackers, porque ese se constituye como el primer paso antes de poder estructurar la nueva tipificación que iría de acuerdo con el vacío legal que actualmente existe en relación a los delitos informáticos

2.4.1 Concepto de Pena

"Sanción, previamente establecida por ley, para quien comete un delito o falta, también especificados."[34]

[34] CABANELLAS, De Torres Guillermo; "Diccionario Jurídico Elemental"; Editorial Heliasta; Edición Decimosexta 2003; Buenos Aires – Argentina; Página 300.

Pena es aquella sanción en la cual se busca sancionar a un culpable de un delito previamente tipificado en la ley penal. La pena será de acuerdo a la medida del acto delictivo y al daño causado a los culpables del delito cometido. Lo primordial para establecer penas al culpable de un hecho, es efectivamente conocer el grado de culpabilidad que tiene el mismo en el delito que cometió.

2.4.2 Culpabilidad

"Es el juicio necesario para vincular en forma personalidad el injusto a su autor, y en su caso, operar como principal indicador del máximo de la magnitud de poder punitivo que puede ejercerse sobre este."[35]

2.4.3 Naturaleza Jurídica de los Delitos Informáticos – Hackers

Tratar de la naturaleza jurídica de los delitos informáticos es referirnos a las características generales que de ellos se desprenden. Los hackers, al ser un tipo de delito informático, también tienen sus características propias, al conocerlas y estudiarlas se va poder especificar el perfil del sujeto activo frente al que nos encontramos, y a su vez vamos a poder establecer el tipo de pena que podemos imponer.

[35] ZAFFARONI, Eugenio Raúl; "Manual de Derecho Penal"; Parte General; Primera Edición; Buenos Aires – Argentina; 2005; Anexo 2.

2.4.3.1 Características de los Hackers

1. Son delitos llamados de “cuello blanco”.
2. El agente debe poseer, al menos un nivel cultural y económico apreciable, se trata de un sujeto activo cualificado por sus conocimientos generales de la informática.
3. Persona muy interesada en el funcionamiento de sistemas operativos.
4. Delincuente silencioso o tecnológico.
5. Son capaces de crear sus propios softwares para entrar a los sistemas.
6. Toma su actividad como un reto intelectual.
7. No tienen reparo en intentar acceder a cualquier máquina conectada a la red, o incluso penetrar a una Intranet privada.
8. Persona experta en materias informáticas.
9. Edad fluctuante entre los 15 y 25 años de edad.
10. Buscan obtener satisfacciones personales y orgullos, basados principalmente en la burla de los sistemas de seguridad dispuestos.

Análisis:

Los hackers son personas con un conocimiento muy alto en sistemas e informática, por lo tanto no pueden ser considerados como un delincuente común que obtendría una rehabilitación social

dentro de un centro de detención. La mayoría de sus actos no buscan causar un daño, sino al contrario buscan una satisfacción personal de acuerdo a lo conocen de la materia. El daño y perjuicio que causan es el "acceder a la información privada de la otra persona", algo que como sabemos se encuentra tipificado en la Carta Magna, es decir la Constitución de la República del Ecuador.

2.4.4 Perfil del Sujeto Activo – Hacker

"Las personas que cometen "Delitos Informáticos" son aquellas que poseen ciertas características que no presentan el denominador común de los delincuentes, esto es, los sujetos activos tienen habilidades para el manejo de los sistemas informáticos y generalmente por su situación laboral se encuentran en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informatizados. Es una persona que "entra" en un sistema informático sin intenciones delictivas. Como consecuencia de los parámetros a seguir por las personas que llevan a cabo este delito, asociamos que poseen características como: listos, decididos, motivados y dispuestos a aceptar un retorno tecnológico. Son características propias que pudieran apreciarse en los empleados del sector de procesamiento de datos. "[36]

2.4.5 Penas Alternativas

Una vez identificado el perfil del sujeto activo, considerado diferente en el caso de los hackers, debido a la característica principal que es la inteligencia informática, resultaría rescatable para la sociedad utilizar este tipo de conocimientos de una manera que contribuya a la sociedad. No es necesario que cada vez que exista un delito la pena sea la prisión o reclusión para el culpable, porque eso no genera, en la mayoría de ocasiones una verdadera rehabilitación social y no contribuye con el mejoramiento de la sociedad por ningún medio.

[36] Lic. Siura L. Arregoitia López, ¨Informática Jurídica¨, Facultad de Derecho. Universidad de La Habana, La Habana – Cuba, 2009, http://www.informatica-juridica.com/trabajos/posibles_sujetos.asp;

Alternativa: Optar o de elegir entre dos cosas diferentes o dos posibilidades de acción.[37]

Es otra opción de la tradicional, o de la estipulada que permite generar nuevas opciones que permitirán obtener mejores resultados específicos de acuerdo a quien se lo aplique.

2.4.6 Posibilidad de nuevas penas

1. Colaborar con sus conocimientos a escuelas fiscales, municipales o de bajos recursos en temas de informática.
2. Contribuir con sus conocimientos en informática en correccionales para colaborar con los adolescentes.
3. Colaborar en las cárceles de mujeres dando charlas sobre informática.
4. Dar charlas en fundaciones de informática.
5. Contribuir realizando murales en parques para mejorar el buen vivir.

Son algunas de las posibilidades que podrían implementarse para sancionar la conducta delictiva de los hackers por su delito cometido, se complementaría uno de los fines del Derecho Procesal Penal, que es resarcir el daño causado, y se debería considerar al tipo de sujeto activo. Obviamente de acuerdo a la magnitud del daño causado se deberá considerar también la posibilidad de la prisión.

[37] Cfr, Mata Carlos, Enciclopedia Jurídica, Concepto de Alternativa, Editorial Torriva, Madrid – España, 2008, Pág. 06.

2.4.7 Casuística

2.4.7.1. Sentencia del Tribunal Constitucional 143/1994, 9 de mayo.

(Sala 1ª. Rec. 3192-1992). Limitación del uso de la informática. Derechos a la intimidad y a la igualdad. Garantías individuales para la protección de las personas en el tratamiento de datos de carácter personal. Sobre el derecho a la intimidad, protección por el uso de la informática, información tributario, y NIF, y si su obligatoriedad y obtención de datos en base al mismo, atenta al derecho constitucional a la intimidad de la persona (Artículo 18 de la Constitución y Real Decreto 338/1990 de 9 de marzo, regulador de la composición y forma del NIF).

Esta Sentencia desestima el recurso de amparo promovido por el Consejo General de Colegios de Economistas de España contra las disposiciones reglamentarias que regularon la composición y la forma de utilización del NIF por considerar vulnerados, entre otros, el art. 18 CE en sus apartados 1 y 4, cita como fuente de interpretación (a tenor del art. 10.2 de la Constitución) el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal de 28 de enero de 1981, y ratificado por España por instrumento de 27 de enero de 1984.

Fundamento jurídico 6º "...en cuanto impone a los Estados firmantes principios específicos de actuación para la obtención de datos, que garanticen la legitimidad de éstos, la adecuación de la información recibida en atención a las finalidades con ellas perseguidas (art. 5); un especial refuerzo de la reserva de datos en materia especialmente conectada con el derecho a la intimidad (art. 6); y la no difusión de datos de carácter personal (art. 7). Todo ello, con el añadido de que las eventuales excepciones que puedan imponerse por cada Estado en las materias y ámbitos

autorizados por el art. 9 del convenio sean única y exclusivamente las necesarias en una sociedad democrática".

El incremento de los medios técnicos de tratamiento de la información puede propiciar la invasión de la vida privada, haciéndose necesario la ampliación del ámbito del juego del derecho a la intimidad, que alcanza a restringir las intromisiones en la vida privada puestas en práctica a través de cualquier instrumento que produzca tal efecto, y a incrementar las facultades de conocimiento y control que se otorguen al ciudadano para salvaguardar el núcleo esencial de su derecho. Las normas autoritarias de recogida de datos, incluso con fines legítimos y de contenido aparentemente neutro, deben incluir garantías adecuadas frente a su uso potencialmente invasor de la vida privada, por lo que si no lo hacen pueden y deben considerarse vulneradoras de la intimidad...

2.4.7.2 Sentencia del Tribunal Constitucional 1 diciembre.

Sobre el derecho a la intimidad personal que consagra el artículo 18.1 de la Constitución.

2.4.7.3. Sentencia del Tribunal Constitucional 106/1998, 18 mayo

Uso de la informática. Libertad Sindical. Garantía de la intimidad.

CAPÍTULO III: CRACKER EN LA LEY PENAL

3.1. DIFERENCIAS Y SIMILITUDES CON EL HACKER

Un gran porcentaje de personas, desconoce los conceptos de los delitos informáticos y por lo tanto desconoce las diferencias típicas entre estos, visión que incide en la imposición de la sanción. Los hackers y los crackers aunque parecen similares no lo son, cada uno tiene sus características propias que los diferencian, pero a su vez poseen similitudes propias de su naturaleza informática. El problema principal para la falta de tipificación es la falta de conocimiento del acto delictivo que cada uno de estos genera a la sociedad cuando ejecutan un delito.

La comisión del delito, -es decir la intencionalidad del cracker de causar daño- no es únicamente el suceso previsto en la ley penal, con la afectación del bien jurídico protegido, sino que ése está rodeado de varias circunstancias, tales como la elección de los medios adecuados para lesionar ese bien, que la conducta a desarrollar no tenga alguna excluyente de responsabilidad o inimputabilidad, que no incidan en el sujeto activo; además de que real y efectivamente se obtenga el daño deseado del bien jurídico. Ya que en caso contrario, podemos estar frente a una conducta que no obstante pretender sea delictuosa no constituya delito por la ausencia de ése, como fin.

De esta circunstancia, se hace necesario que el acto delictivo cometido por el cracker, lesione el bien jurídico protegido y que el sujeto activo, sea quien cometa el delito previamente tipificado en la ley penal.

3.1.1 Diferencias

Las diferencias entre uno y otro las podemos distinguir básicamente en sus características, y estas son:

3.1.1.1 Hacker

- Sujeto activo: Adicto.
- Perfil criminológico del sujeto activo: Fanático de la programación.
- Intencionalidad del sujeto activo y del acto delictivo: Ingresar al sistema informático y operativo.
- Tipo de sujeto activo: Usuario.
- Perfil del tipo de sujeto activo: Usuario que está entregado a la programación y a las tecnologías informáticas.
- Por el resultado dañoso de su accionar: Dolo intencional.
- Acto delictivo: Reto personal.

3.1.1.2 Cracker

- Sujeto activo: Destructor.
- Perfil criminológico del sujeto activo: Pirata informático.
- Intencionalidad del sujeto activo y del acto delictivo: Producir daños en el sistema informático y operativo.
- Tipo de sujeto activo: Persona.
- Perfil del tipo de sujeto activo: Persona que es capaz de reventar las protecciones que tienen los programas o aplicaciones.
- Por el resultado dañoso de su accionar: Dolo preterintencional.
- Acto delictivo: Causar daño.

Como se observa las diferencias entre cada uno de ellos, son totalmente claras, mientras el primero busca una satisfacción personal para demostrar sus conocimientos en informática y es considerado como un fanático de los sistemas informáticos que solamente busca acceder por simple ego natural sin causar daño al sistema; el segundo busca causar daño y acceder al sistema informático, a la información privada, es un programador que se lo conoce como “pirata informático”.

“La infracción dolosa, que es aquella en que hay el designio de causar daño, es: intencional, cuando el acontecimiento dañosa o peligroso, que es el resultado de la acción o de la omisión de que la ley hace depender la existencia de la infracción, fue previsto y querido por el agente como

consecuencia de su propia acción u omisión; y, preterintencional, cuando de la acción u omisión se deriva un acontecimiento dañoso o peligroso más grave que aquel que quiso el agente…"[38]

Estas diferencias serán la base para poder tipificar la conducta, diferenciar al sujeto pasivo e incluso identificar al verbo rector y bien jurídico protegido, así como la intención del daño y el acto delictivo provocado. A continuación vamos a exponer las similitudes entre estos dos tipos de delitos informáticos, y estos son:

3.1.2 Similitudes

3.1.2.1 Hacker - Cracker

1. Realizan actos que se consideran delictivos.
2. Tienen relación con la informática, Internet, electrónica y sistemas.
3. Son realizados por personas naturales.
4. Ambos ingresan a la información privada de otras personas sin autorización.
5. No se encuentran tipificados, ni diferenciados en el Código Penal Actual.

[38] Código Penal; Libro 1 De las Infracciones de las Personas Responsables de las Infracciones y de las Penas en General; Título II De las Infracciones en General; Capítulo I De la Infracción Consumada y de la Tentativa; Art. 14.- Infracción dolosa, culposa, intencional y preterintencional; Página 3.

La principal similitud que se encuentra entre los dos, es que el acto delictivo cometido por el sujeto activo, sea este hacker o cracker, no está tipificado como tal dentro del Código Penal actual, y esto genera un vacío legal que origina inseguridad jurídica, toda vez que las víctimas se ven limitadas en el ejercicio pleno de sus derechos frente a estos delitos. Como vemos existen similitudes y diferencias claramente expuestas entre estos dos delitos que nos permitirán a lo largo de este trabajo realizar un análisis de las clases de delitos.

3.2 TIPIFICACIÓN ACTUAL

La tipificación que se puede encontrar -más afín a la conducta delictiva y al delito cometido por lo crackers- dentro de la legislación nacional, es la establecida en la ley penal, que expresa:

- **"**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 contenidos en un sistema de información o red electrónica, será reprimido con prisión de seis meses o 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."[39]

[39] Código Penal; Título V De los Delitos contra la Seguridad Pública; Capítulo VII Del Incendio y Otras Destrucciones, De los Deterioros y Daños; Art. … (415.1).- Daños informáticos; Pagina 79.

Análisis:

- Sujeto Activo.- Cracker.
- Sujeto Pasivo.- Cualquier persona u Organismo público o privado.
- Bien Jurídico Protegido.- Inviolabilidad de la información contenida en programas, bases de datos, o cualquier mensaje de datos contenidos en un sistema de información o red electrónica.
- Verbos rectores: Destruir, alterar, inutilizar, suprimir o dañar.
- Forma.- Temporal – Definitiva.
- Pena.- Prisión de seis meses a tres años.
- Multa.- Sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

Análisis agravante, inciso segundo:

- Agravante.- Que los sistemas informáticos o redes estén destinados a prestar un servicio público o estén vinculados con la defensa nacional.
- Pena – Agravada.- Prisión de tres a cinco años.
- Multa – Agravada.- Doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.
- Bien Jurídico Protegido.- La inviolabilidad de programas, bases de datos, información o cualquier mensaje de datos contenidos en un sistema de información o red electrónica.

La intención de causar daño y estropear el sistema informático es lo que permite el cometimiento o ejecución del acto delictivo, cuyo modus operandi, se origina cuando el cracker accede a la información, con el fin de destruir el sistema informático y violar la privacidad y la intimidad de las personas, destacando que al hablar de información, nos referimos a cualquier tipo de información sin importar la identidad de la persona afectada.

El cracker al ser catalogado como un "destructor informático" busca causar daños, como vemos en este concepto:

"Destructor. Argot informático, del entorno Internet, con el que designamos a la persona que es capaz de reventar las protecciones que tienen los programas o aplicaciones. También se puede llamar cracker al pirata informático capaz de entrar en redes de seguridad y producir daños en el sistema."[40]

Por lo expuesto, el delito por el cracker, se adecua a la normativa penal referida, -pudiendo ser esta la ley con la cual se sancionará al culpable del hecho.

[40] CULTURA S.A.; "Diccionario de Informática"; Editorial Grafilles; Edición 1999; Madrid – España; Página 75.

3.3. TRATAMIENTO JURÍDICO

3.3.1. Problemas para la Conceptualización

Dentro del tratamiento jurídico que realizaré sobre el delito que comete el cracker como sujeto del mismo, primero estableceré la problemática que existe dentro de los tratadistas para diferenciar y conceptualizar el tipo de delito informático. El tratadista Español Salazar Cano dentro de su análisis a la problemática que existe en el mundo para conceptualizar y diferenciar a cada tipo de delito informático, realiza un análisis a tres características esenciales de estos, que son:

1. Los sujetos activos cracker no se encuentran sectorizados en una sola actividad, son de carácter amplio y general, debido a que la informática se aplica en numerosos sectores de la actividad socioeconómica.

2. Su unidad viene dada por la originalidad técnica impuesta por el fenómeno informático.

3. Es un delito complejo porque los aspectos técnicos de la informática en su interrelación con el Derecho, recae sobre diversas ramas o especialidades jurídicas.[41]

Para contribuir a mejorar esta problemática, el pasado 23 de noviembre, el Consejo de Ministros del Interior de los Estados que conforman la Unión Europea, conjuntamente con Estados Unidos, Sudáfrica, Canadá y Japón firmaron en Budapest "La Convención sobre Delitos Informáticos", con el objetivo de ayudar al complimiento de la justicia.

[41] Cfr, Análisis realizado por el tratadista Español Salazar Cano, "Derecho Informático Penal".

En el Titulo 1 de esta Convención se conceptualiza temas acerca de los delitos informáticos, y el cracking es:

"Cracking: Uso inapropiado de programas informático y sistemas de cómputo, que comprende sabotaje y daños ocasionados a equipos informáticos."[42]

Considero que para el Ecuador sería un gran avance adoptar este tipo de conceptualización dada para el delito cometido por el cracker, para poder identificar al mismo, como sujeto activo de delito.

3.3.2. Bien Jurídico Protegido en el Acto Delictivo Del Cracker

El bien jurídico protegido dentro del acto delictivo realizado por el cracker es la inviolabilidad de la información contenida en programas, bases de datos, o cualquier mensaje de datos contenidos en un sistema de información o red electrónica. El concepto de bien "es todo aquello que sirve para satisfacer una necesidad humana, material o espiritual, y es jurídico cuando está protegido por una norma legal."[43]

Y el concepto de interés "es la posición del sujeto respecto al bien que es idóneo para la satisfacción de una necesidad."[44]

[42] Convención sobre Delitos Informáticos; 23 de noviembre de 2010; Consejo de Ministros de Interior – Budapest; Titulo 1 "Delitos contra la Confidencialidad, Integridad y Disponibilidad de Datos y Sistemas de Computo".

[43] LABAFUT, Gustavo; "Derecho Penal Tomo II"; Editorial Jurídica de Chile; Actualizado por el Profesor Julio Zenteno Vargas; Santiago – Chile; Sexta Edición; 1977; Página 8.

[44] Ibidem.

Por lo tanto podemos entender que lo que realmente tutela el derecho no son los bienes, la cosa en sí sino al hombre, en cuanto tiene necesidad de ellas, o sea, lo que tutela es el interés, que es el objeto de la tutela penal, en cuanto ese interés es lesionado por el delito, pasa a constituir el objeto jurídico del delito. En base a este análisis el cracker ha lesionado el derecho constitucional, que dice:

"Se reconoce y garantizará a las personas:

21.- El derecho a la inviolabilidad y al secreto de la correspondencia física y virtual: esta no podrá ser retenida, abierta ni examinada, excepto en los casos previstos en la ley, previa intervención judicial y con la obligación de guardar el secreto de los asuntos ajenos al hecho que motiva su examen. Este derecho protege cualquier tipo o forma de comunicación…"[45]

3.3.3 Sujeto Activo – Cracker

Una vez identificado el bien jurídico que lesiona el acto delictivo cometido por el cracker, ahora voy a identificar el perfil de la persona que comete el delito informático. Personas que se introducen en sistemas remotos con la intención de destruir datos, denegar el servicio a usuarios legítimos, y en general a causar problemas.

El Pirata informático. Tiene dos variantes:

1. El que penetra en un sistema informático y roba información o se produce destrozos en el mismo.

[45] Constitución de la República del Ecuador; Título II Derechos; Capítulo Sexto; Derechos de Libertad; Artículo 66; Página 55.

2. El que se dedica a desproteger todo tipo de programas, incluidas versiones shareware para hacerlas plenamente operativas como de programas completos de tipo comercial, que presentan protecciones anti-copia.

Cracker es aquel Hacker fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas. Para los grandes fabricantes de sistemas este grupo es el más rebelde de todos, ya que siempre encuentran el modo de romper las protecciones tecnológicas. Pero el problema no radica ahí, si no en que esta violación es difundida normalmente a través de la Red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers.

En la actualidad es habitual ver como se muestran los Cracks de la mayoría de Software de forma gratuita a través de Internet, a fin de formar parte de la red, para ser difundidos a través de otros grupos, cuyo estudio detallara más adelante. Hemos manifestado que Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware; por lo que es fácil comprender que un Cracker debe conocer perfectamente las dos caras de la tecnología, esto es la parte de programación y la parte física de la electrónica.

Su finalidad, es romper y violar las protecciones y otros elementos de seguridad de los programas comerciales, en su mayoría con el fin de sacar provecho de los mismos en el mercado negro, creando códigos para utilizarlos en la copia de archivos. Sus acciones pueden ir desde la destrucción de información ya sea a través de virus u otros medios, hasta el robo de datos a fin de venderlos para obtener réditos. Ejemplo de su actuar ilegal son los millones de CDs con softwares piratas que circulan por el mundo entero y de hecho, muchas personas no llegan a sospechar que parte del soft que tienen en sus máquinas, incluso con certificados de garantía de

procedencia, es craqueado. Esto sucede sobre todo en los países del tercer mundo, donde se agrupan en pequeñas compañías y contratan especialistas de alto nivel.

Aunque tratan de cubrir sus actividades ilícitas, con el ropaje de la aventura y el desafío tecnológico, los miles y millones de pérdidas y los cientos de casos que conoce anualmente la policía y fiscales de todo el mundo, hablan de un creciente índice delictivo, por los pecuniarios que representa, lo que sobrepasa el interés técnico científico en el área de la informática. Las herramientas de este espécimen suelen ser potentes editores hexadecimales y debuger's mediante los cuales "desmontonan" los programas, lo que se conoce como ingeniería inversa hasta llegar a las protecciones que son generalmente utilidades de tiempo que se representan en el reloj interno de la máquina o en el sistema operativo para desencadenar una cuenta regresiva que descontará los días posibles a usar el software hasta que el mismo caduque y el usuario este obligado a pagarlo o renunciar a él.

Es importante puntualizar que debe diferenciarse entre quienes utilizan este sistema sofisticado como un negocio para su beneficio personal, mediante el uso de técnicas delincuenciales, de aquellas personas carentes de recursos que "craquean" un programa para su uso; debiendo señalar que la principal condición para que florezca el negocio del cracking es el precio, siempre en ascenso y en algunos casos exorbitantes, de los programas de mayor utilidad en contraposición con el del hardware que ha mantenido una tendencia decreciente, por lo que no es de extrañar que con frecuencia el costo del software que soporta una máquina, aun una de última generación, sea superior al de ésta.[46]

[46] Página de Internet: http://www.informatica-juridica.com/trabajos/posibles_sujetos.asp; elaborado por Lic. Siura L. Arregoitia López Facultad de Derecho. Universidad de La Habana.

3.3.4. Nuevas Figuras Típicas Del Cracker

Además del cracker que comete un tipo de delito específico, actualmente existen nuevas figuras típicas que se relacionan con la conducta típica del cracker, se las podía considerar con una subclasificación de este tipo de delito informático.

- Crackers de sistemas: término designado a programadores y decoders que alteran el contenido de un determinado programa, por ejemplo, alterando fechas de expiración de un determinado programa para hacerlo funcionar como si se tratara de una copia legítima.

- Crackers de Criptografía: término usado para aquellos que se dedican a la ruptura de criptografía (cracking codes).

- Phreaker: cracker especializado en telefonía. Tiene conocimiento para hacer conexiones gratuitas, reprogramar centrales telefónicas, grabar conversaciones de otros teléfonos para luego poder escuchar la conversación en su propio teléfono, etc.

- Cyberpunk: son los vándalos de páginas web o sistemas informatizados. Destruyen el trabajo ajeno.

Estos podrían considerarse como agravantes dentro de una nueva tipificación en la legislación nacional.

3.4. PENAS ALTERNATIVAS Y CASUÍSTICA

3.4.1. Penas Alternativas

Para que exista la posibilidad de penas alternativas considero que se hace necesario diferenciar la concurrencia de personas que intervienen en este tipo de delito informático.

3.4.1.1 Autores

- Ejecutor: Es el que ejecuta el hecho o el que toma parte en la ejecución. Se convierte en el autor directo, que actúa de tres tipos:

  a.- Autor individual: Cuando ejecuta la conducta descripta en el tipo penal.

  b.- *Coautor:* Cuando varios realizan paralelamente la conducta típica, es decir, entre varios se reparten la tarea, y cada uno hace un aporte indispensable al hecho.

- Determinador: El que determina o manda u otro a cometer el hecho.

Autor mediante determinación:

a.- Autor directo: Cuando se vale de otro que no realiza la conducta delictiva.

b. Autor mediato**:** Cuando se vale de otro que actúa sin tipicidad objetiva, sin dolo y actúa justificadamente.

Autor de determinación:

Es el autor de un tipo independiente. No es autor del delito, sino de la determinación de otro a provocar una mutación típica del mundo, cuando el otro, no realiza la conducta delictiva, realiza una conducta típica pero justificada.

3.4.1.2. Participes

Participe mediante determinación (Instigador): Es el que determina al hecho a otro que comete un injusto, (conducta típica y antijurídica) y comete un delito (conducta típica, antijurídica y culpable).

- Auxiliador o Cooperador**:** Participe mediante auxilio o cooperación, son los que prestan al autor o autores auxilio, ayuda o cooperación, y pueden ser:

a) Cómplices necesarios o primarios: Los que prestan una cooperación o auxilio sin el cual el hecho no hubiera podido cometerse, pero no pueden ser autores debido a que no tiene los caracteres típicos del autor.

b) Cómplices secundarios: Los que cooperan de cualquier otro modo en la ejecución del hecho, prestan ayuda posterior al hecho cumpliendo promesas anteriores al mismo.

De acuerdo a esta clasificación para determinar el grado de culpabilidad del sujeto activo dentro del delito cometido por el cracker, es necesario diferenciar el tipo de participación de cada persona, debido a que para la culminación del delito sea hace necesario que intervengan varias personas, y es primordial diferenciar la conducta delictiva de cada una, para a su vez se sancione con la respectiva pena o multa a las mismas.

3.4.2. Casuística

Cracking: Primera sentencia por ataque DDos en España. (J. de lo Penal. Num.2 de Lleidal S., 07-02-06)

El condenado actuó (tras ser expulsado de un foro por no respetar el código de conducta) contra un servidor informático provocando el colapso de millones de ordenadores tanto en Europa como en Asia, sobre todo en China. Se trata del autor del mayor ataque DDos (Distributed Denial of Service) en España, que llegó a afectar en algunos momentos al 30% de los internautas españoles, unos 3 millones de usuarios según la Unidad de Delitos Telemáticos de la Guardia Civil. Este internauta, apodado en la red bajo los nick de `Ronnie´ y `Mike 25´ ha sido condenado a dos años de prisión por delitos de daños continuados, valorados en 1.332.500 euros

de responsabilidad civil, desglosados en: 474.500 € en daños a LLEIDA.NET 570.716 € en daños a WANADOO 120.000 € en daños a ONO 218.000 € en daños a IRC-HISPANO Además deberá pagar 18 meses de multa con una cuota diaria de 6€. Este es el primer caso que culmina en sentencia por ataque de denegación de servicio en España, y posiblemente el de mayor cuantía en una sentencia relativa a temas informáticos.

3.4.2.1 Cracking: Por un blindaje legal contra los ciberataques

"Uno de los bienes más preciados que tiene una sociedad es el progreso científico y tecnológico. Sin dudas, de un tiempo a esta parte, el avance tecnológico ha dominado la escena del mundo. Y la construcción de la gran madeja de comunicación e información en la que se transformó Internet pareciera ser la protagonista estelar de esta gran historia. Tanto, que la revista Wired Italia lanzó a fines del pasado año el proyecto Internet for peace, con el único fin de postular a la red para el Nobel de la Paz 2010. La delirante idea, que fue apoyada por el diseñador italiano Giorgio Armani, el científico Humberto Veronesi, la activista y Nobel de Paz Shirin Ebadi y la empresas Sony Ericsson y las divisiones italianas de Microsoft y Vodafone, sostiene como argumento principal que Internet permite la construcción de un mundo pacífico.

Como es sabido, el progreso permitió el acceso al mundo aunque también trajo aparejado una sofisticación en el uso y abuso de las herramientas técnicas. Muchas de ellas fueron beneficiosas para las empresas y, otras tantas, fulminantes. Los fraudes, robos y sabotajes fueron lentamente ganando su espacio y alertando a las firmas sobre la necesidad de proteger su organización de la delincuencia informática.

A comienzos de este año se lanzó desde China el ataque más profesional y estratégico que haya vivido en la historia de la red. La Operación Aurora, como se la denominó, aprovechó vulnerabilidades para asestar su gran golpe, que persiguió un sólo destino: robar información. El operativo, puso en guardia a todas las empresas de software así como a las de aplicaciones de seguridad para cerrar las brechas y evitar el peligro de contaminar a millones de usuarios en todo el mundo.

Por su parte, el reciente estudio del gigante Symantec proporciona valiosos datos acerca del estado de la seguridad de la información en el ámbito empresarial a nivel mundial, con algunas particularidades del mercado latinoamericano. De acuerdo al reporte State of Enterprise Security 2010 el 75% de las empresas encuestadas manifestaron haber sufrido algún tipo de ataque informático en los 12 meses anteriores a la encuesta, cifra que alcanza el 49% cuando se analiza la región latinoamericana. Entre los blancos más recurrentes cabe destacar la sustracción de datos personales o de información sobre tarjetas de crédito de los clientes, como así también el robo de propiedad intelectual.

Los ciberataques, cada vez más frecuentes y más certeros, generan cuantiosas pérdidas económicas, afectando, adicionalmente, la productividad de las empresas, la confianza de los clientes y la reputación e imagen de la empresa en el mercado. Además, ponen de manifiesto la importancia de resguardar el know how, los secretos comerciales, la propiedad intelectual y las bases de datos de clientes, proveedores y empleados, que conforman una parte importante del capital de una empresa. Acaso su capital intangible. Afortunadamente, existen recursos humanos y tecnológicos para hacer frente a los ciberataques. Pero, es importante que las empresas consideren que cuentan también con herramientas legales que les permiten prevenir el robo de información o reducir los daños provocados por la delincuencia informática. La seguridad de la información requiere de la coordinación de tres pilares básicos: lo humano, lo tecnológico y lo legal.

El Nobel parece demasiado si tenemos en cuenta que ese galardón recayó en manos de la Madre Teresa de Calcuta o Nelson Mandela. El espacio que se ha ganado Internet dentro de la historia es otro. El ahora es hoy. Y la batalla no es contra la pobreza estructural si no contra los delincuentes que no permiten que el progreso llegue cada vez a más personas."[47]

3.5. ANÁLISIS GENERAL

Los crackers son delincuentes informáticos que causan daño a sus víctimas, a diferencia de los hackers que solamente acceden a la información para saciar sus ansias de conocimientos; los crackers buscan dañar ya sea la información, como el sistema informático, aparte de acceder a la información privada ajena. La principal característica del acto delictivo proveniente de los crackers es la intromisión y destrucción de los sistemas operativos de propiedad de empresas públicas o privadas. Surgen en la actualidad nuevos delincuentes como los crackers, quienes cometen sabotajes, fraudes, espionaje, violación de derechos intelectuales, etc., y generan daño al titular del derecho violado y a la sociedad por la constante inseguridad que generan.

Dentro de este escenario es aplicable una paradoja del poder y del control, en donde mientras más sofisticado se torna un sistema, más vulnerable se vuelve; pero de la misma manera lo que se vuelve transcendental es generar nuevas o modificar las leyes para evitar el cometimiento de más daños a la sociedad.

[47] Cfr. Mota, Cristian, ¨Análisis criminológico de los delincuentes informáticos¨, 2010, Santiago – Chile, http://www.delitosinformaticos.com/06/2010/delitos/por-un-blindaje-legal-contra-los-ciberataques

CAPÍTULO IV: PHISHING EN LA LEY PENAL

4.1. DIFERENCIAS Y SIMILITUDES ENTRE EL HACKER Y CRACKER

El phishing es el tipo de delito informático menos conocido y menos estudiado a nivel internacional y por lo tanto nacional. La gran mayoría de delitos cometidos por phishing se confunde con los otros tipos de delitos informáticos, que son más conocidos sus efectos delictivos. Al contrario de lo que sucede con el hacker y el cracker, poco o nada se conoce del delito y daño que se comete a través del phishing al enviar un correo electrónico para pescar o robar la información personal.

Para estructurar las diferencias que existen entre el hacker y el cracker con el phishing se hace fundamental, individualizar la conceptualización sobre este, debido al gran desconocimiento del concepto, así como del ilícito que cometen al enviar el email con el virus y del acto delictivo que ocasionan. El inicio del ilícito se genera al enviar un correo electrónico a la lista de contactos o a un correo electrónico en específico. Como es conocido por todos, cuando una persona crea un correo electrónico dentro de un servicio de Internet sean estos hotmail, gmail, yahoo, entre otros; no se especifica en ningún momento algún tipo de requisito legal que nos permita identificar de

alguna manera al creador; pero lo que si podemos es realizar un rastreo de quien es la persona que envío el correo electrónico, que se convierte en el sujeto activo y en el responsable del acto delictivo.

Para empezar con las diferencias entre el hacker, cracker y el phishing es importante conocer que el phishing puede considerarse como una clasificación del fraude informático, y así es como lo constituyen las entidades bancarias privadas o públicas.

Las diferencias entre estos delitos informáticos, son claramente identificables debido al daño, al dolo y al perjuicio que causan a sus víctimas. Lo importante es ubicar el acto delictivo que realiza el sujeto activo para configurarlo dentro de la tipología propia a fin de sancionar esta conducta. A continuación detallaré algunas de las semejanzas de estos delitos:

4.1.1 Semejanzas Hacker – Cracker – Phishing

- Son delitos informáticos.
- Son realizados por personas naturales.
- Tienen relación con la informática, electrónica, Internet y los sistemas operativos.
- Violan el derecho a la intimidad de las personas.
- No se encuentran tipificados en el Código Penal, ni en ninguna ley dentro de la Legislación Nacional.
- Utilizan la informática para la realización de sus ilícitos.

- No se conoce sus conceptos, características y daños que causan.
- Necesitan un experto para identificar la magnitud del perjuicio que causan.
- Existe nexo causal entre el autor y el acto delictivo.
- Se debe identificar el acto delictivo que comete cada uno de ellos (hacker, cracker y phishing) para determinar la sanción.

Las semejanzas que existen entre estos constituyen los parámetros iniciales para poder identificar estas conductas como delitos informáticos y establecer una descripción típica, que permita diferenciar estos tres tipos delictivos, que deberán estar ubicados en el capítulo correspondiente. Las circunstancias que rodean el acto delictivo y el perjuicio que éste ocasiona a sus víctimas, son consideraciones fundamentales para determinar el tipo de sanción que corresponde a cada uno.

4.2. TIPIFICACIÓN ACTUAL

El phishing es el tipo de delito informático que tiene como objetivo robar la información personal de una persona, lo que se configura a través de un actuar doloso. La forma de consumación del delito se produce cuando se envía un correo electrónico a un grupo de personas o persona determinada, imitando logos, sellos, etc., de una institución sea pública, privada o bancaria, en la cual se busca que la víctima ingrese claves personales, las mismas que serán de inmediato copiadas o pescadas (phishing) por los delincuentes informáticos y procederán a finalizar el ilícito.

"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 una pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica."[48]

Análisis del Texto Legal

- Sujeto Activo.- Hacker – cracker – phishing.
- Sujeto Pasivo.- Cualquier persona – entidad pública o privada.
- Objetivo.- Obtener información sobre datos personales de otros.
- Verbo Rector 1.- Ceder, publicar, utilizar, trasferir información a cualquier título.
- Bien Jurídico Protegido.- Inviolabilidad de la Información contenida en soportes informáticos, computacionales o automatizados.
- Pena.- Prisión de dos meses a dos años.
- Multa.- Mil a dos mil dólares de los Estados Unidos de Norteamérica.

En este artículo podemos ver que el objetivo del acto delictivo del phishing que se encuentra tipificado, es: obtener información sobre datos personales de otros, el medio utilizado es la obtención ilícita. Por otra parte, en el verbo rector 3, se determina que la obtención ilícita tiene un fin que no es otro que utilizar la información**,** -es decir enviar el correo electrónico falso-, que le permite robar a la víctima. Pero, más allá del uso que el phishing haga con la información

[48] Código Penal,; Título II De los Delitos contra las Garantías Constitucionales y la Igualdad Racial; Capítulo V; De los Delitos contra la inviolabilidad de Domicilio; Artículo 202.2.- Delitos contra la Información Protegida, Página 40.

obtenida, es preciso resaltar que su obtención transgrede varios derechos constitucionales, ya que no existe la autorización de su titular.

4.3. TRATAMIENTO JURÍDICO

Para este tipo de delito informático, vamos a realizar un análisis de los principios rectores en la interpretación de los documentos electrónicos, que dentro de este tipo de delito informático es primordial tratarlo.

4.3.3 Principios rectores en la interpretación de los documentos electrónicos

Son cuatro principios los cuales sirven para la interpretación de documentos electrónicos, dentro de éstos consta el correo electrónico que se convierte en el medio de realización de este delito informático.

4.3.1.1. Principio de los Equivalentes Funcionales

Tanto el proyecto de ley, como la ley de Modelo de la CNUDMI emplean el criterio de los equivalentes funcionales, por medio del cual se estudian las finalidades, los propósitos y las funciones aplicables al análisis del contenido y el soporte de los documentos que constan sobre el papel, para así llegar a fijar la forma con la que se pueden aprobar tales requisitos por medio de las nuevas tecnologías y sistemas electrónicos.

4.3.1.2. Principio de Integridad

Se presume que el mensaje de datos recibido corresponde al enviado; por cuanto una vez ha sido firmado digitalmente, si se llegará a modificar cualquier parte del mismo, a través de los sistemas técnicos se puede comprobar tal cambio, por lo tanto, se tiene como presunción legal que el mensaje recibido corresponde al enviado y, en caso dado de considerarse que ha sido modificado, el onus probandi está en manos del interesado, quien, en tal evento, deberá probar que las normas de seguridad establecidas no fueron respetadas.

Integridad, significa que la información enviada a través del mensaje de datos no carece de alguna de sus partes, así como que tampoco ha sido transformada. En tal sentido, la integridad es uno de los requisitos esenciales con los cuales se otorga plena validez jurídica al documento electrónico y es por esto que se confía en la firma digital o en la firma electrónica.

Integridad del mensaje de datos que ha sido firmado adecuadamente, y es además, totalmente independiente el medio en que se almacene.

4.3.1.3. Principio de la Inalterabilidad

Este principio guarda una estrecha relación con el anterior, pues hace referencia a que si bien el contenido del mensaje de datos se puede llegar a alterar, la firma para el caso en que se utilice este medio: firma electrónica, o digital, permite demostrar que tal evento ha ocurrido y, por lo tanto, que dicho mensaje de datos carece de valor real, o cuando es falso o ha sido alterado.

4.3.1.4. Principio de Autenticidad

En el mismo contexto que la firma manuscrita, se presume que la firma digital pertenece exclusivamente a la persona que consta como titular de un certificado digital. En la utilización de un sistema que utilice el mecanismo de firma digital, cada parte de la relación se encuentra determinada, habida cuenta de que la clave privada empleada en la emisión de la firma digital sólo puede estar siendo empleada por quien es su propietario.

4.3.2. Principio de Validez

Para que el correo electrónico tenga validez jurídica es necesario que previamente cumpla con una serie de requisitos legales, que le otorguen dicha validez. Los requisitos legales serán los tomados del Artículo 6 de la Ley 527 de 1999 Española, los mismos que nos servirán para valorar a los correos electrónicos que envié el phishing para el cometimiento del ilícito; y son:

4.3.2.1. Escrito

"Cuando una norma requiera que la información conste por escrito, ese requisito quedara satisfecho con un mensaje de datos, siempre y cuando la información que contenga sea accesible para posterior consulta."[49]

[49] RINCON, Cárdenas Erick; "Manual de derecho electrónico y de Internet"; Colección Lecciones de Jurisprudencia Central; Editorial Universidad de Rosario; Primera Edición; Bogotá D.C. – Colombia; Página 53.

De acuerdo a este requisito un correo electrónico que contenga información escrita será un documento con completa validez jurídica que actué como prueba para comprobar un ilícito.

4.3.2.2. Original

"Cuando una norma requiera que la información sea presentada en su forma original, ese requisito se satisface si cumple los siguientes requisitos:

- Que pueda garantizarse que la información se ha conservado íntegra desde se generó por primera vez.

- Que al requerirse que la información sea presentada, ésta pueda ser mostrada a quien deba presentarse."[50]

4.3.2.3. Integridad

"Se considerará que la información consignada en un mensaje de datos es íntegra si ha permanecido completa e inalterada, o si se ha adicionado algún endoso o cambio que sea inherente o propio de su mismo proceso de comunicación, archivo o presentación."[51]

[50] Ibidem.

[51] Ibidem; Página 53 – 54.

Para que estos requisitos legales se puedan utilizar como Doctrina Jurídica Internacional durante una investigación, se requiere además conceptos de correo electrónico dentro de la Legislación Nacional y mecanismos con los cuales se pueda llegar a rastrear a quien envió él mismo.

4.3.3. Concepto de Correo Electrónico

"El correo electrónico nos permite enviar cartas escritas con el computador a otras personas que tengan acceso a la Red."[52]

4.3.4. Características Del Correo Electrónico

1.- Casi instantáneo.

2.- Se puede enviar un correo a cualquier parte del mundo.

3.- Es necesario tener una conexión a Internet.4.- Es necesario tener una cuenta de Correo Electrónico.

[52] Fiscalía General del Estado; "Manual de Manejo de Evidencias Digitales y Entornos Informáticos"; Dirección Nacional de Tecnología de la Informática; Página 20.

4.3.5. Rastreo Del Correo Electrónico

"Al enviar un correo electrónico, la computadora se identifica con una serie de números al sistema del proveedor de servicios de Internet (ISP). Enseguida se le asigna una dirección IP y es dividido y en paquetes pequeños de información a través del protocolo TCP/IP. Los paquetes pasan por una computadora especial llamada servidor (server) que los fija con una identificación única (Message-ID) posteriormente los sellan con la fecha y hora de recepción (Sello de tiempo). Más tarde al momento del envió se examina su dirección de correo para ver si corresponde la dirección IP de alguna de las computadoras conectadas en una red local (dominio). Si no corresponde, envía los paquetes a otros servidores, hasta que encuentra al que reconoce la dirección como una computadora dentro de su dominio, y los dirige a ella, es aquí donde los paquetes se unen otra vez en su forma original a través del protocolo TCP/IP. (Protocolo de Control de Transparencia y Protocolo de Internet). Siendo visible su contenido a través de la interfase gráfica del programa de correo electrónico instalado en la máquina destinataria."[53]

"Hay que tomar en cuenta que los correos electrónicos se mantienen sobre un servidor de correo, y no en la computadora del emisor o del destinatario, a menos que el operador los guarde allí. Al redactarlos se trasmiten al servidor de correo para ser enviados. Al recibirlas, nuestra computadora hace una petición al Servidor de correo, para que los mensajes sean trasmitidos luego a la computadora del destinatario, donde el operador la puede guardar o leer y cerrar. Al cerrar sin guardar, la copia de la carta visualizada en la pantalla del destinatario desaparece, pero se mantiene en el servidor, hasta que el operador solicita que sea borrada."[54]

"En algunas ocasiones es necesario seguir el rastro de los Correos Electrónicos enviados por el Internet. Los rastros se graban en el encabezamiento del e-mail recibido. Normalmente, el

[53] Ibidem.

[54] Ibidem.

encabezamiento que aparece es breve. La apariencia del encabezamiento está determinada por el proveedor de servicios de Internet utilizado por nuestra computadora, o la de quien recibe el correo electrónico. Para encontrar los rastros, se requiere un encabezamiento completo o avanzado, posibilidad que existe como una opción en nuestro proveedor de servicios de Internet."[55]

Este rastreo lo realizan peritos expertos de la Fiscalía o de la Policía Judicial, con lo que se permite identificar a quien envió el correo electrónico, viola la privacidad de la víctima y roba o copia la información de la misma. Dentro de la Fiscalía General del Estado ya se realiza este tipo de investigaciones, las cuales si se aplican conjuntamente con la modificación y nueva regulación de las leyes, seria formidable para obtener la tan anhelada justicia.

Analizar el rastreo que se puede dar al correo electrónico, es la base para la estructura del delito que llega a cometer el phishing, a diferencia de lo que realizamos con el hacker y cracker, por cuanto como lo hemos expresado el correo electrónico es el punto de partida de esta conducta ilícita.

4.4. Penas Alternativas y Casuística

El phishing no es un experto en sistemas como lo es un hacker, no es un adicto como lo es cracker, es un ladrón cibernético con la única misión de robarse la información que tiene la persona por medio del correo electrónico. El problema y el trabajo que tiene el Legislador es encontrar como se puede expedir un régimen legal general sustitutivo de penas para quienes sean reos de un tipo de delito informático.

[55] Ibidem.

El análisis que expondré a continuación es basado en el estudio del Ab. Jorge Sosa Meza, en el cual expresa que el criterio que debe utilizarse es el de proporcionalidad, en el cual se realiza la siguiente trilogía:

- La infracción es una hipótesis ideal.
- El acto típico contemplado por la norma penal para el sujeto infractor en general.
- La pena o sanción, la misma que también puede ceder excepcionalmente ante determinados sujetos que fundamentalmente se presumen inintencionados o inconscientes del acto dañoso.

Para nuestro estudio esta relación de proporcionalidad se convierte en la primera que existe entre el delito tipificado y la sanción que corresponde al ilícito.

4.4.1. Criterio de Proporcionalidad

La proporcionalidad debe también existir entre la ejecución de la sanción, con la propia sanción o pena y con el sujeto activo a quien se aplica la sanción. La ejecución de una pena puede sustituirse cuando se trate de sujetos que, por situaciones especiales de vulnerabilidad puedan ser objeto de una desigualdad y en consecuencia producir efectos negativos en su integridad física y psicológica, en relación especifica con los sujetos activos de los delitos informáticos pueden ser considerados como “situaciones especiales”, de ahí él porque de estas algunas penas alternativas que propongo para sancionar.

4.4.2. Situaciones Especiales

Algunas de las posibilidades a utilizarse como solución a la grave situación que existe actualmente dentro del sistema carcelario a nivel nacional, para sancionar al autor del delito informático, específicamente del phishing, algunas pueden ser:

- Multa proporcional de acuerdo a la magnitud del daño causado a la víctima.
- Arresto los fines de semana un equivalente en proporción al tiempo que debería el sujeto activo estar en prisión permanente.
- Localización permanente del reo y que realice sus actividades con mediana normalidad. Se puede rastrear a los reos por medio de dispositivos electrónicos para obtener una localización permanente de estos.
- El sometimiento a programas de recuperación, mediante los cuales el reo de un delito informático, podrá utilizar los conocimientos de informática e Internet a Instituciones que lo aprovecharan para bien.

Lo que constituye esta posibilidad de nuevas penas es primero, descongestionar el sistema carcelario actual, y segundo la rehabilitación y reinserción del individuo a la sociedad.

El phishing no solamente envía un correo electrónico ficticio, además se desconoce lo que realice con la información que llega a tener de la víctima, lo que confirma que actúa con

inminente mala fe. La teoría en la que se basa este tipo de delito es la "Teoría del Resultado, en la cual hay que juzgar de acuerdo al hecho dañoso que produjo el daño."[56]

Para establecer si se puede plantear penas alternativas es fundamental plantear la "conducta" de quien comete phishing, para esto analizaremos la misma.

4.4.3. Conducta

"Se trata de un concepto jurídico limitado por datos ópticos. Es un hacer voluntario final. Tiene un aspecto interno (proposición del fin y selección de los medios), y un aspecto externo (puesta en marcha de la causalidad)."[57]

La conducta es sinónimo de acción y de acto. La omisión no existe como forma de acción o de conducta, sino que antes del tipo todas son acciones. Sin el tipo no se distinguen las omisiones del no hacer. Lo principal que debe existir para que la conducta sea imputada a un individuo en particular, es la existencia del nexo causal y en este caso en particular se produce cuando al rastrear el correo electrónico se encuentra a la persona que lo envió.

[56] Notas Personales.

[57] VACA Andrade, Ricardo; "Manual del Derecho Procesal Penal"; Tomo 1; Corporación de Estudios y Publicaciones; Cuarta Edición; 2009; Anexo 2.

4.4.2. Casuística

La casuística con la cual se puede hacer un análisis de los phishing, es la española, porque como ya lo hemos conocido y estudiado es la que se encuentra actualmente con mayor evolución a nivel mundial en aspectos informáticos.

Este hecho sucedió en España y fue expuesto a nivel mundial el día 13 de julio del año 2010, y específica:

"La compañía aérea Spanair ha lanzado una promoción por la cual ofrecía a sus clientes un viaje gratis por cada tres que hubiera realizado con su compañía. Sin embargo, el pasado día 7 de Julio, Spanair publicó un comunicado urgente en el que informaba a todos sus usuarios de la existencia de un ataque de phishing, con el siguiente texto:

Si recibís un email con un remitente promocion@spanair.com, asunto "Billete promoción: FW: felicidades has ganado un billete de Spanair por ser cliente de Spanair, que tiene el aspecto que os adjuntamos y os remite a esta web http://spanair-promo.com.web.es-es.greenhouse.cl/.%20/.es-promo/fare.action.php, por favor, no deis vuestros datos se trata de phishing. Para los que no sabéis que es el phishing os informamos de que es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito…Para luego ser usados de forma fraudulenta. Estamos trabajando para solucionar el problema con la mayor celeridad. Nuestra web funciona con total normalidad. ¡Muchas gracias por vuestra comprensión! ¡Seguiremos informando sobre el tema!

Sin embargo, hoy mismo han vuelto a sufrir dicho ataque, por lo que la compañía ha reiterado el comunicado a través de su web: De nuevo e-mails de suplantación. El tema es el mismo de la semana pasada, la única diferencia es que esta vez viene de direcciones diferentes: la página es esta: http://web3.adams-hosting.net/.%20%20/ y os remite a esta web http://spanair-promo.com.web.es-es.unitel.tv.bo/.%20%20/.es/index.htm.

Por favor, no deis vuestros datos. De nuevo se trata de phishing. Para los que no sabéis que es el phishing os informamos de que es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito para luego ser usados de forma fraudulenta. Ya hemos tomado las medidas oportunas. Importante: os recordamos que nuestra página web donde podéis comprar billetes de forma absolutamente segura funciona con total normalidad. www.spanair.com."[58]

Se lo establece como tratamiento no consentido y delimitación de la responsabilidad subjetiva. (T.S.S, 05-06-04).

"Contratos de ejecución de campañas de marketing. El responsable de la infracción por tratar datos sin el consentimiento del afectado es el titular del fichero. La posición de la empresa es subsumible en la definición legal de «responsable del tratamiento» en cuanto decide sobre la finalidad, contenido y uso del tratamiento. Y en cuanto tal, le es imputable la infracción descrita en el artículo 44.3. de la Ley Orgánica España relativa al tratamiento de datos y la utilización del fichero sin las garantías legalmente previstas, por haber vulnerado la exigencia del previo consentimiento del afectado establecida en el artículo 6.1 de la propia Ley Orgánica 15/1999. La regulación de la Ley 15/1999, de Protección de Datos de carácter personal distingue ya perfectamente entre responsable del fichero y responsable del tratamiento, y uno y otro se hallan sujetos al régimen sancionador establecido en el título VII de dicha Ley." [59]

[58] Spanair, Empresa Turística, Madrid – España, 2010 ¨Robo de Identidad de su página web¨, http://www.delitosinformaticos.com/07/2010/noticias/spanair-sufre-un-ataque-de-phising

[59] Notas Personales; Información obtenida de la Legislación de España.

4.5. ANÁLISIS GENERAL

El phishing tiene la capacidad de ejecutar el hecho ilícito en contra de una o varias de personas las cuales pueden existir dentro de la lista de sus contactos electrónicos, o en específico a una persona, a quien el delincuente informático buscará realizar el acto ilícito. La Fiscalía General del Estado como la Institución que será quien realiza las investigaciones dentro del proceso penal y que busca elementos de convicción para determinar un culpable y al responsable del hecho delictivo, ya cuenta con el "Manual de Manejo de Evidencias Digitales y Entornos Informatices", emitido por la Dirección Nacional de Tecnología de la Información; el mismo que solamente necesita aplicar conjuntamente con una tipificación objetiva real dentro de la Legislación Nacional.

El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, a una amenaza potencial antes desconocida, de ahí el porqué de una modificación notoria en la Legislación Nacional.

CAPÍTULO V: FRAUDE INFORMÁTICO EN LA LEY PENAL

5.1 DIFERENCIAS Y SIMILITUDES CON EL HACKER, CRACKER Y PHISHING

El fraude informático es el delito informático más conocido en el Ecuador, debido a que ha avanzado de manera prominente dentro del ámbito criminal. Al fraude informático se lo considera como el delito más grande, ya que afecta a una mayor cantidad de personas a nivel nacional. Actualmente los fraudes informáticos han avanzado en gran medida, debido a que las entidades bancarias y las entidades gubernamentales han creado páginas de Internet para que los usuarios realicen por este medio las actividades, con esto los delincuentes han “progresado” sus actos delictivos por esta vía.

5.1.1 Diferencias

5.1.1.1 Hacker

1. Fanático; 2. Utiliza sus conocimientos; 3. No daña al sistema: 4. No utiliza la información; 5. Reto personal; 6. Se satisface personalmente; 7. Tiene conocimientos acerca de informática por sus estudios.

5.1.1.2 Cracker

1. Destructor; 2. Utiliza su ingenio; 3. Daña al sistema; 4. Utiliza medios ilícitos; 5. Viola la privacidad y causa daño a la víctima; 6. Delito más dañino dentro de la informática; 7. Tiene conocimientos empíricos.

5.1.1.3. Phishing

1. Ladrón; 2. Utiliza medios informáticos; 3. Roba al sistema informático; 4. Utiliza el correo electrónico; 5. Es un usuario de la Web; 6. Conoce de informática; 7. Roba la información a sus contactos.

5.1.1.4. Fraude informático

1. Estafador; 2. Utiliza su astucia; 3. Obtiene información del sistema; 4. Abusa de la confianza; 5. Delito más conocido dentro del Ecuador; 6. Busca engañar; 7. Frustra a la ley.

Las diferencias entre estos cuatro tipos de delitos informáticos realizada a lo largo del presente plan de investigación demuestra nuevamente, la necesidad imperante de buscar una tipificación propia y específica para cada tipo de conducta criminal, pues como hemos apreciado, pese a que todos son delitos informáticos no son iguales.

“El fraude informático abarca dos vertientes principales:

- Acceso y manipulación de los datos.
- Manipulación de los programas.

Además manifiesta que el fraude informático, como uno de los principales exponentes del delito informático, el fin que persiguen dentro de seis apartados, estos son:

- Manipulación en los datos e informaciones contenidas en los archivos o soportes físicos informáticos ajenos.
- Acceso a los datos y/o utilización de los mismos por quien no está autorizado para ello.
- Introducción de programas o rutinas en otros ordenadores para destruir información, datos o programas.

- Utilización del ordenador y/o los programas de otra persona, sin autorización, con el fin de obtener beneficios propios y perjuicio de otro.
- Utilización del ordenador con fines fraudulentos.
- Agresión a la "privacidad" mediante la utilización y procesamiento de datos personales con fin distinto al autorizado."[60]

A continuación voy a exponer las similitudes que existen entre estos tipos de delitos informáticos:

5.1.2 Similitudes entre Hacker – Cracker – Phishing – Fraude Informático

- Son delitos informáticos.
- Utilizan la informática, sistemas, electrónica y el Internet para realizar sus actos.
- Son realizados por personas contra otras personas.
- Violan varios principios procesales penales.
- No se encuentran tipificados en la Ley Penal correspondiente.
- No son muy conocidos dentro de la sociedad ecuatoriana.

Estos cuatro tipos de delitos informáticos son de acción pública, por lo tanto deberán sujetarse al trámite establecido para estos delitos en el Código de Procedimiento Penal. Son delitos que

[60] DAVARA, Miguel Ángel; "Manual de Derecho de Informático"; Editorial Aranzadi; Sexta Edición; 2004; Páginas 354 – 355.

necesitan una tipificación individualizada objetiva y subjetiva dentro de la Legislación Nacional. Las similitudes que hemos expuesto a lo largo de los capítulos anteriores y en este, demuestran que en la actualidad se hace prioritario la tipificación de estos delitos informáticos, como ya se lo ha hecho en otras Legislaciones como, la española, argentina, chilena, entre otras; y, el Convenio del Cybercrimen, el mismo que es firmado por los países que conforman la Unión Europea, entre los años 2004 y 2005.

5.2 TIPIFICACIÓN EN EL CÓDIGO PENAL

El fraude informático al ser considerado como el delito más conocido dentro de la Legislación Nacional, es que en gran medida puede apegarse a lo que actualmente se encuentra tipificado en el Código Penal actual. Además de esta tipificación podemos encontrar la Ley de Comercio Electrónico, la cual se utiliza como una ley auxiliar al momento de sancionar a un culpable.

Estos son los artículos que están tipificados en el Código Penal: **"**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 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 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, estas 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."[61]

Análisis:

- Sujeto Activo.- Cualquier persona.
- Sujeto Pasivo.- Cualquier persona.
- Bien Jurídico Protegido.- Información privada.
- Verbo rector 1.- Acceder a la información protegida.
- Verbo rector 2.- Acceder a la seguridad nacional.
- Verbo rector 3.- Divulgar información.
- Sujeto Activo - Agravante.- Personas que custodian el servicio de información.
- Penas.-
- Verbo rector 1.- Prisión de seis meses a un año.
- Verbo rector 2.- Prisión de uno a tres años.
- Verbo rector 3.- Reclusión menor ordinaria de tres a seis años.
- Agravante.- Reclusión menor de seis a nueve años.

[61] Código Penal; Título II De los Delitos contra las Garantías Constitucionales y la Igualdad Racial; Capítulo V; De los Delitos contra la Inviolabilidad de Domicilio; Artículo 202.1.- Delitos contra la Información Protegida; Pagina 40.

- Multas.-
- Verbo rector 1.- Quinientos a mil dólares de los Estados Unidos de Norteamérica.
- Verbo rector 2.- Mil a mil quinientos dólares de los Estados Unidos de Norteamérica.
- Verbo rector 3.- Dos mil a diez mil dólares de los Estados Unidos de Norteamérica.
- Agravante.- Dos mil a diez mil dólares de los Estados Unidos de Norteamérica.

Esta tipificación que se encuentra actualmente en la Legislación, se puede considerar como el primer paso para sancionar al sujeto activo que comete fraude informático. En el último inciso el verbo rector que encontramos es acceder a la información para divulgarla, y esta información es custodiada por este, por consiguiente se apega en gran medida con el delito que comete quien realiza fraude informático, porque como ya lo expusimos el concepto es:

"Delito que comete el encargado de vigilar intereses públicos o privados, cuando se confabula con los contrarios."[62]

Por lo tanto, podemos considerar que existe una tipificación del fraude informático, a diferencia de lo que ocurre con los demás tipos de delitos informáticos.

"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,

[62] SANCHEZ, Osvaldo; "Diccionario Enciclopédico Universal del Ecuador"; Editorial Geosistemas; Bogotá, Colombia; Tomo 1; 1993; Página 449.

serán sancionadas con una pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica."[63]

Análisis:

- Sujeto Activo.- Cualquier persona.
- Sujeto Pasivo.- Cualquier persona.
- Verbo Rector 1.- Obtener información sobre datos personales de otros.
- Verbo Rector 2.- Ceder información.
- Verbo Rector 3.- Publicar información.
- Verbo Rector 4.- Utilizar la información.
- Verbo Rector 5.- Transferir la información a cualquier título.
- Bien Jurídico Protegido.- Información contenida en soportes informáticos, computacionales o automatizados.
- Pena.- Prisión de dos meses a dos años.
- Multa.- Mil a dos mil dólares de los Estados Unidos de Norteamérica.

Este artículo podemos considerarlo como la tipificación actual del fraude informático. Cumple en esencia con los dos postulados fundamentales para constituir este delito, y son:

[63] Código Penal,; Título II De los Delitos contra las Garantías Constitucionales y la Igualdad Racial; Capítulo V; De los Delitos contra la inviolabilidad de Domicilio; Artículo 202.2.- Delitos contra la Información Protegida, Página 40 .

1. Abuso de confianza

2. Engaño, como la causa del delito.

Este es el único tipo de delito informático que se considera tipificado dentro de nuestra Legislación. Además contamos con la Ley de Comercio Electrónico, que en concordancia con el Código Penal, encontramos que tipifica lo siguiente:

“Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros. La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.”[64]

Se garantiza que la información informática es de carácter personal, por lo tanto ninguna persona, sin previa autorización del titular de la misma puede hacer uso de esta, para cualquier tipo de actividad. La nueva tipificación que se puede hacer acerca del fraude informático, deberá buscar que abarque todos los postulados que existen, para lograr abarcar todos los puntos de vista de los delincuentes informáticos.

[64] Ley de Comercio Electrónico; Art. 9.

5.3 TRATAMIENTO JURÍDICO

Al existir un tipo de tipificación del fraude informático, para la realización del presente trabajo de investigación, también seguiremos con la temática de los anteriores delitos, con la tipificación objetiva, la estructura del delito y los principios penales que serán la base para la nueva tipificación.

5.3.1 Tipificación Objetiva

Para considerar al fraude informática y empezar con la tipificación objetiva, se utiliza el "Manual de Manejo de Evidencias Digitales y Entornos Informáticos", al considerar a la informática como el principal instrumento del cometimiento de este delito.

"La informática es un instrumento o herramienta cuando es usada como medio para cometer una infracción penal."[65]

1. Sujeto Activo: Persona que comete el delito, abusa de la confianza y engaña al dueño de la información.

2. Sujeto Pasivo: Persona que confía la información informática y es engañada. – cualquier persona – entidad pública o privada.

[65] Fiscalía General del Estado; "Manual de Manejo de Evidencias Digitales y Entornos Informáticos"; Dirección Nacional de Tecnología de la Informática; Página 7.

3. Verbo rector: Es la base con la cual se tipifica al delito y al daño que causan. – engañar y robar la información informática.

4. Bien Jurídico Protegido: "Su esencia consiste en la relación de disponibilidad de un sujeto con un objeto."[66] – información privada.

Además de esta tipificación objetiva, no podemos olvidar de lo que se encuentra actualmente tipificado en el Art. 202.1 y en el Art. 202. 2, por consiguiente en la nueva tipificación se debe considerar sobremanera lo que ya está en la ley.

5.3.2 Estructura del Delito – Fraude Informático

1.- Por la gravedad: "Son infracciones los actos imputables sancionados por las leyes penales, y se dividen en delitos y contravenciones, según la naturaleza de la pena peculiar."[67]

Fraude informático se convierte el delito, al estar tipificado objetivamente, a diferencia de lo que sucede con los demás tipos de delitos informáticos, con lo cual se reafirma el Art. 10 del Código de Procedimiento Penal.

[66] ZAFFARONI, Eugenio Raúl; "Manual de Derecho Penal"; Parte General; Primera Edición; Buenos Aires, Argentina; 2005, Página 369.

[67] Código Penal; Título II De las Infracciones en General; Capítulo I De la Infracción Consumida y de la Tentativa; Artículo 10.- Infracciones.

2.- Por su naturaleza en el ejercicio de la acción penal: "Desde el punto de vista de su ejercicio, la acción penal es de dos clases: pública y privada."[68]

El delito de fraude informático, podrá ser iniciado por parte del Estado, representado por parte de la Fiscalía General, esta será la vía pública; mediante la área de la Tecnología de la Información y la Comunicación.

3.- Por su estructura: El fraude informático es simple lesiona un solo bien jurídico protegido, no llega a constituirse como complejo. La información es un instrumento para la configuración del delito, porque se utilizan para romper las seguridades de un sistema, en base al abuso de confianza y al engaño para el cometimiento del ilícito.

4.- Por el resultado que produce: El resultado que produce el fraude informático es de tipo material debido a que los actos son realizados por personas con conciencia y voluntad, por lo tanto imputables y tendrá repercusión en el futuro.

5.- Por la duración: De entre la clasificación pertinente, el fraude informático se constituye como permanente. Permanentes, porque su consumación puede durar un lapso de tiempo largo, según el daño causado al bien protegido (información, software, hardware). El fraude informático es permanente porque roba la información privada y este bien jurídico protegido es posible que no se pueda recuperar y el daño causado sea permanente.

[68] Reformas al Código de Procedimiento Penal; Quito, Martes 24 de Marzo del 2009 – N 155; Registro Oficial Suplemento; Artículo 32.- Clasificación Acción Penal; Página 3.

6.- Por sus efectos: Pueden ser de dos clases, y en este caso en particular es el daño. Daño, por la afectación del bien jurídico tutelado. Se constituye como daño lesionar y afectar la información privada, que es el bien jurídico protegido.

7.- Por el bien jurídico protegido: Es un delito económico, porque al constituirse el bien jurídico protegido la información privada, quienes lo realizan son considerados delincuentes de cuello blanco, porque actúan de acuerdo a los conocimientos adquiridos de la informática, sistemas, electrónica e Internet.

5.3.3 Principios del Proceso Penal

1.- Principio de Legalidad: Todo debe estar predeterminado en la ley.

2.- Principio de Necesidad: Debe establecerse oficialmente la existencia o inexistencia de la infracción y la magnitud del daño causado, para sancionar al culpable.[69]

3.- Principio de Derecho a la Intimidad: Podemos conceptualizar al derecho de la intimidad como el "derecho de las personas a poseer información privada propia, la misma será utilizada de acuerdo a la necesidad del dueño de la misma"[70]

El derecho a la intimidad previsto en la Constitución Política de la República, para efectos de esta Ley, comprende también el derecho a la privacidad, a la confidencialidad, a la reserva, al secreto sobre los datos proporcionados en cualquier relación con terceros,

[69] Notas personales.

[70] Notas personales.

a la no divulgación de los datos personales y a no recibir información o mensajes no solicitados.

4.- Principio de Lesividad: Es otro principio que se constituye fundamental dentro de los delitos informáticos, para el tratamiento jurídico de estos.

"Verifica la afectación, por daño o peligro concreto, de un bien jurídico en forma significativa, y el alcance de la norma debe estar limitado por otras de igual o superior jerarquía."[71]

5.4 Penas Alternativas y Casuística

5.4.1 Penas Alternativas

El fraude informático tiene una característica propia, que lo constituye como único dentro de los tipos de delitos informáticos que es el abuso de confianza. Debido a esta característica, el perfil criminológico del sujeto activo, será analizado de acuerdo a la ciencia empírica de la criminología, de esta manera:

"Colisión de deberes, abuso de confianza; Actúa con conciencia; Actúa con voluntad; Actúa con conocimiento."[72]

[71] Notas personales.

[72] Notas personales.

De acuerdo a este análisis el sujeto activo se convierte en imputable de un delito de fraude informático, por esto la posibilidad de plantear penas alternativas no se hace posible. Las penas alternativas se consideran como una segunda opción para sancionar al culpable de un delito, de acuerdo a la magnitud del daño que han causado a sus víctimas. El delito de fraude informático, no tiene esta posibilidad, debido a que quien realizo el ilícito, tiene una característica específica, la cual confirma que actuó con dolo, esta es el abuso de confianza y el engaño.

5.4.2 Casuística

1.- Varios casos de fraude informático: “Estas conductas consisten en la manipulación ilícita, a través de la creación de datos falsos o la alteración de datos o procesos contenidos en sistemas informáticos, realizada con el objeto de obtener ganancias indebidas. Los distintos métodos para realizar estas conductas se deducen, fácilmente, de la forma de trabajo de un sistema informático: en primer lugar, es posible alterar datos, omitir ingresar datos verdaderos o introducir datos falsos, en un ordenador. Esta forma de realización se conoce como manipulación del input.

´

Ulrich Sieber, cita como ejemplo de esta modalidad el siguiente caso tomado de la jurisprudencia alemana: Una empleada de un banco del sur de Alemania transfirió, en febrero de 1983, un millón trescientos mil marcos alemanes a la cuenta de una amiga -cómplice en la maniobra- mediante el simple mecanismo de imputar el crédito en una terminal de computadora del banco. La operación fue realizada a primera hora de la mañana y su falsedad podría haber sido detectada por el sistema de seguridad del banco al mediodía. Sin embargo, la rápida transmisión del crédito a través de sistemas informáticos conectados en línea (on line), hizo posible que la amiga de la empleada retirara, en otra sucursal del banco, un millón doscientos ochenta mil marcos unos minutos después de realizada la operación informática.

En segundo lugar, es posible interferir en el correcto procesamiento de la información, alterando el programa o secuencia lógica con el que trabaja el ordenador. Esta modalidad puede ser cometida tanto al modificar los programas originales, como al adicionar al sistema programas especiales que introduce el autor. A diferencia de las manipulaciones del input que, incluso, pueden ser realizadas por personas sin conocimientos especiales de informática, esta modalidad es más específicamente informática y requiere conocimientos técnicos especiales.[73]

5.4.2.1 Caso de la Jurisprudencia Alemana

"Sieber, el autor, empleado de una importante empresa, ingresó al sistema informático un programa que le permitió incluir en los archivos de pagos de salarios de la compañía a «personas ficticias» e imputar los pagos correspondientes a sus sueldos a una cuenta personal del autor.

Esta maniobra hubiera sido descubierta fácilmente por los mecanismos de seguridad del banco (listas de control, sumarios de cuentas, etc.) que eran revisados y evaluados periódicamente por la compañía. Por este motivo, para evitar ser descubierto, el autor produjo cambios en el programa de pago de salarios para que los «empleados ficticios» y los pagos realizados, no aparecieran en los listados de control.

Por último, es posible falsear el resultado, inicialmente correcto, obtenido por un ordenador: a esta modalidad se la conoce como manipulación del output. Una característica general de este tipo de fraudes, interesante para el análisis jurídico, es que, en la mayoría de los casos detectados, la conducta delictiva es repetida varias veces en el tiempo. Lo que sucede es que, una

[73] Notas Personales.

vez que el autor descubre o genera una laguna o falla en el sistema, tiene la posibilidad de repetir, cuantas veces quiera, la comisión del hecho. Incluso, en los casos de «manipulación del programa», la reiteración puede ser automática, realizada por el mismo sistema sin ninguna participación del autor y cada vez que el programa se active. En el ejemplo jurisprudencial citado al hacer referencia a las manipulaciones en el programa, el autor podría irse de vacaciones, ser despedido de la empresa o incluso morir y el sistema seguiría imputando el pago de sueldos a los empleados ficticios en su cuenta personal. Una problemática especial plantea la posibilidad de realizar estas conductas a través de los sistemas de teleproceso. Si el sistema informático está conectado a una red de comunicación entre ordenadores, a través de las líneas telefónicas o de cualquiera de los medios de comunicación remota de amplio desarrollo en los últimos años, el autor podría realizar estas conductas sin ni siquiera tener que ingresar a las oficinas donde funciona el sistema, incluso desde su propia casa y con una computadora personal. Aún más, los sistemas de comunicación internacional, permiten que una conducta de este tipo sea realizada en un país y tenga efectos en otro.

Respecto a los objetos sobre los que recae la acción del fraude informático, estos son, generalmente, los datos informáticos relativos a activos o valores. En la mayoría de los casos estos datos representan valores intangibles (ej.: depósitos monetarios, créditos, etc.), en otros casos, los datos que son objeto del fraude, representan objetos corporales (mercadería, dinero en efectivo, etc.) que obtiene el autor mediante la manipulación del sistema. En las manipulaciones referidas a datos que representan objetos corporales, las pérdidas para la víctima son, generalmente, menores ya que están limitadas por la cantidad de objetos disponibles. En cambio, en la manipulación de datos referida a bienes intangibles, el monto del perjuicio no se limita a la cantidad existente sino que, por el contrario, puede ser «creado » por el autor.”[74]

[74] Notas personales.

5.5 Análisis General

El fraude informático es considerado como el delito macro, el más grande o el más conocido de entre los tipos de delitos informáticos, además de ser el único que en gran medida se encuentra tipificado actualmente en la Ley Penal; y tiene su base fundamental en el engaño y en el abuso de confianza. Dentro del fraude informático se busca verificar la afectación, por daño o peligro concreto, del bien jurídico por medio del abuso de confianza y el engaño por parte del sujeto activo al o los sujetos pasivos. Cuando una persona comete el delito de fraude informático, es preciso que actúe con dolo, si no existe esta característica, no hay delito y por lo tanto no hay el designio de causar daño.

CAPÍTULO VI: PROPUESTAS NUEVAS TENDENCIAS EN LA TIPIFICACIÓN DE LOS DELITOS INFORMÁTICOS

6.1 ANEXO AL CÓDIGO PENAL

Art… Daño Informático: Se impondrá pena de localización permanente al reo por el periodo de tres a seis años al que por cualquier medio accede, borre, suprima, modifique o inutilice, sin autorización, los datos registrados en una computadora.

Art… Abuso de medios informáticos: Sera sancionado con la pena de tres a seis años de prisión, a quien sin autorización o cediendo la que se le hubiere concedido, intercepte, interfiere en su uso o permita que otra use en perjuicio de terceros o del Estado, un sistema o red de computadoras o de telecomunicaciones, un programa de computación o de telecomunicaciones, un soporte lógico, una base de datos, o cualquier otra aplicación informática de telecomunicaciones o telemática.

Art…Estafa informática: Se impondrá prisión de tres a doce años a la persona que, con la intención de procurar u obtener un beneficio patrimonial para sí o para un tercero, influya o manipule el ingreso, procesamiento o el resultado de los datos de un sistema de cómputo, mediante programación, empleo de datos falsos o incompletos, uso indebido de datos o cualquier otra acción que incida en el proceso de los datos del sistema.

Art… Espionaje informático*:* Se impondrá prisión de tres a seis años al que se apodere, interfiera, transmita, copie, modifique, destruya, utilice, impida, o recicle datos de valor para el tráfico económico de la industria y el comercio. La pena se aumentará en un tercio si son datos de carácter político, relacionados con la seguridad del Estado.

Art… Uso de virus (software malicioso): Se impondrá pena de tres a seis años de prisión al que produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional virus (software malicioso), u otro programa de computación de efectos dañinos.

Art… Clonación de páginas electrónicas (páginas web): Se impondrá prisión de tres a seis años siempre que no se trate de una conducta sancionada con una pena más grave, al que diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas clonadas de una original previamente existente.

Art… Suplantación de sitios web para capturar datos personales (phishing): *Se* impondrá pena de prisión de tres a seis años siempre que la conducta no constituya delito sancionado con pena más grave, a quien capture datos personales para beneficio propio o de un tercero, suplantando sitios de la red de internet o por cualquier otro medio informático. Si el acto causa perjuicio la pena se aumentará en un tercio.

Art… Sabotaje informático: Se impondrá pena de tres a seis años de prisión, al que destruya, altere, entorpezca o inutilice un sistema de tratamiento de información, sus partes o componentes lógicos, una base de datos o un sistema informático, o impida, altere, obstaculice o modifique su funcionamiento sin autorización.

- La pena será de prisión de cuatro a ocho años, cuando:

a) Como consecuencia de la conducta del autor sobreviniere peligro o daño común. Siempre que la conducta no se encuentre más severamente sancionada.

b) Si la conducta se realizare en provecho propio o de un tercero, por parte de empleado o contratista del sistema informático o telemático o por un servidor público.

c) Si contienen datos de carácter público.

d) El que emplee medios tecnológicos que impidan a personas autorizadas acceder a la utilización lícita de los sistemas o redes de telecomunicaciones, sin estar facultado.

Art… Agravante: Seguridad Nacional: El monto de las penas incluidas en esta ley serán duplicadas cuando el resultado de cualquiera de los delitos informáticos aquí contemplados afecte negativamente la seguridad nacional.

CONCLUSIONES

1. El hacker, cracker, phishing y el fraude informático constituyen tipos de delitos informáticos, con conceptualizaciones y características propias; una vez diferenciado cada uno de ellos, se puede diferenciar a los sujetos activos, sujetos pasivos, verbos rectores y los bienes jurídicos protegidos; para a su vez poder tipificar y sancionar a los culpables de estos delitos.

2. En la Legislación ecuatoriana actual, existen tipificaciones acerca de los delitos informáticos, dentro de esto tenemos a la tipificación del fraude informático, como un tipo macro de delito, el cual busca abarcar a todo lo referente a los daños informáticos; pero el principal problema que logre encontrar dentro de esta investigación, es la falta de diferenciación que obviamente existe entre cada uno de los tipos de delitos, algo que ya lo realizan otras legislaciones.

3. No se puede catalogar a los delincuentes informáticos, como un delincuente común, porque como lo observamos a lo largo del desarrollo de este trabajo, son personas con un perfil intelectual más alto que otro tipo de delincuentes, debido a que tienen un conocimiento elevado de informática – sistemas – Internet y electrónica lo que les

permite estar un paso más alto y por consiguiente que el Ecuador se implante para ellos penas alternativas.

4. Para el Ecuador sería transcendental y generaría un paso muy hacia el mejoramiento de tratamiento jurídico de los delitos informáticos el tener dentro del Código Penal actual, un capítulo especialmente dedicado a este tipo de delitos, dentro del cual se diferencian conceptos, sujetos, verbos rectores y se podría sancionar al culpable de acuerdo a rango de culpabilidad.

RECOMENDACIONES

1. La posibilidad que el Ecuador debería tomar en cuenta es la de adherirse a Convenios Internacionales, específicamente a los europeos, los mismos que ya diferencian nuevos tipos de delitos informáticos, conociendo conceptos, diferencias, tipificándolos, de acuerdo a esto se podría ubicar al culpable del delito informático en cualquier lugar del mundo; porque como es conocido este tipo de delincuentes se manejan mediante redes internacionales que les permite permanecer en el anonimato.

2. La posibilidad de la reforma al Código Penal, se plantea como primordial y beneficiaria notablemente al sistema penal ecuatoriano, debido a que los culpables de delitos informáticos se encuentran impunes dentro de nuestra sociedad, porque como es conocido no existe hasta el día de hoy un culpable en las cárceles que haya cometido un delito informático, mientras que al contrario existen cientos de víctimas de delitos informáticos que no han sido retribuidas por el daño que sufrieron.

3. Además considero que sería importante que existan en el Ecuador varios expertos sobre temas informáticos y que a su vez contribuyan dentro de la investigación para lograr la determinar el grado de culpabilidad de acuerdo al tipo de delito de los culpables.

BIBLIOGRAFÍA

1.- LEYES Y CÓDIGOS:

- Código de Procedimiento Penal, Ley s/n, Registro Oficial 360-S, de fecha 13 de enero 2000.
- Código Penal, Registro Oficial –S 147, de fecha 22 de enero de 1971.
- Constitución de la República del Ecuador, Registro Oficial 449, 20 de Octubre 2008.
- Ley Orgánica de Transparencia y Acceso a la Información – Ecuador, Registro Oficial 367, de fecha 23 julio de 1998.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos – Ecuador, Ley 2002-67, Registro Oficial 557, de fecha 17 de abril de 2002.
- Reformas al Código Penal y al Código de Procedimiento Penal, Registro Oficial 805, de fecha 26 de marzo de 2010.

2.- LIBROS:

- CISNEROS, Germán; "**Metodología Jurídica**"; Librería Jurídica Cevallos; Primera Edición; Quito-Ecuador; 2003.

- ROMEO CASABONA, Carlos María; "**La Protección Penal de los Mensajes de Correo Electrónico y de Otras Comunicaciones de Carácter Personal a través de Internet**"; Catedrático de Derecho Penal; Universidad del País Vasco.

- ANARTE BORRALLO, Enrique; "**Sobre los Límites de la Protección Penal de Datos Personales**"; Profesor de Derecho Penal; Universidad de Huelva.

- REYNA ALFARO, Luis Miguel; "**El Bien Jurídico en el Delito Informático**"; Abogado, Director de la Revista Electrónica de Derecho Penal.

- GALVIS TRASLAVIÑA, Carlos Mauricio; "**Introducción a la Tarjeta con Banda Magnética**".

- MUÑOZ ESQUIVEL, Oliver; "**La Convención sobre Delitos Informáticos**".

- CUADRADO RUIZ, María Ángeles; "**La Responsabilidad Penal de las Personas Jurídicas. Un paso hacia adelante… ¿Un paso hacia atrás?**"; Profesora Titular de Derecho Penal; Universidad de Granada.

- STERLING, Bruce; "**La Caza de los Hackers**".

- HIMANEN, Pekka; "**La Ética del Hacker y el Espíritu de la Era de la Informática**".

- REINOSO TORRES, Héctor; "**Investigación Bibliográfica**"; Segunda Edición, año 2002; Quito – Ecuador.

- SOLANO, Orlando; "**Manual de Informática**".

- GUERRERO, María Fernanda y Otros; "**Penalización de la Criminalidad Informática**"; Ed. Gustavo Ibáñez, Bogotá, 1998.

- VIEGA, María José; "**Un Nuevo Desafío Jurídico: Delitos Informáticos**"; Ed. Mc Graw – Hiu, México, 1996.

- ASENSIO, Pedro Alberto de Miguel; "**Derecho Privado de Internet**"; Tercera Edición Actualizada Civitas; Año 2002; Madrid – España.

- PEÑA VALENZUELA, Daniel; "**Aspectos Legales de Internet y del Comercio Electrónico**"; Ediciones Dupre Ltda.; Año 2001; Colombia.

3.- PÁGINAS DE INTERNET:

- http://www.delitosinformaticos.com/11/2006/propiedad-intelectual/una-juez-de-santander-sentencia-que-la-descarga-de-musica-por-internet-no-es-delito

- http://publicaciones. derecho.org/redp

- http://www.20minutos.es/noticia/ 174327/0/ musica/descargas /legales/

- http://www.20minuto s.es/noticia/ 167999/0/ internet/ sentencia/ p2p/

- http://www.pagina12.com.ar/diario/sociedad/3-64873-2006-03-29.html

- http://www.clarin.com/diario/2006/04/25/um/m-01184112.htm