Universidad Andina Simón Bolívar - Universidad del Azuay
Universidad Técnica "José Peralta"

ESPECIALIDAD EN DERECHO PROCESAL

ASIGNATURA DEL TRABAJO: INFORMATICA JURIDICA

DELITOS INFORMATICOS

DIRECTOR: Dr. Juan Peña Aguirre

Realizado por: Fernando Sigüenza Vintimilla

DEDICATORIA

A MI MADRE, QUE CON MUCHO CARIÑO, AMOR Y RESPETO ME HA SABIDO GUIAR EN LA VIDA, FORJANDO UN HOMBRE CONVALORES Y FE , PARA CONSEGUIR CADA UNO DE LOS LOGROS TRAZADOS POR LOS DOS. PUES CON CADA UNA DE SUS ACTUACIONES FORJO MIS ESTUDIOS, Y ME LLEVO A SER UN HOMBRE A SU IMAGEN LLENA DE FE, ESPERANZA Y AMOR.

AGRADECIMIENTO

UN AGRADECIMIENTO A LAS UNIVERSIDADES

UNIVERSIDAD ANDINA SIMÓN BOLÍVAR –

UNIVERSIDAD DEL AZUAY

UNIVERSIDAD TÉCNICA "JOSÉ PERALTA",

POR LA CALIDAD DELA ESPECIALIDAD

QUE IMPARTIERON CADA UNO DE LOS CATEDRATICOS.

INDICE DE CONTENIDOS

TRABAJO DE TITULACION PREVIO ALAGRADUACION DE LA ESPECIALIDAD DE DERECHO PROCESAL

RESUMEN

En este trabajo se pretende realizar un análisis de los delitos informáticos en nuestra legislación, así como los reglamentos existentes. Realizar un análisis del avance tecnológico ha sido la última década, así como nuevas formas de cometer delitos en el mundo y nuestro país. Formas de evitarlos, la prevención y las nuevas técnicas para prevenir la comisión de los delitos cibernéticos en nuestro país. Estudiar las técnicas y métodos para que la información en nuestro computador no sea filtrado, además un análisis de toda la información digital que puede ser objeto de cambio y alteración, con fines delictivos y de índole ilegal.

ABSTRACT

THIS PAPER INTENDS TO CONDUCT AN ANALYSIS OF COMPUTER CRIMES IN OUR LEGISLATION AND EXISTING REGULATIONS. PERFORM AN ANALYSIS OF TECHNOLOGICAL ADVANCE HAS BEEN THE LAST DECADE AND NEW WAYS TO COMMIT CRIMES IN THE WORLD AND OUR COUNTRY. WAYS OF AVOIDING, PREVENTING AND NEW TECHNIQUES TO PREVENT THE COMMISSION OF CYBER CRIME IN OUR COUNTRY. STUDY THE TECHNIQUES AND METHODS SO THAT THE INFORMATION IN OUR COMPUTER IS NOT FILTERED, ALSO A ANÁISIS OF ALL DIGITAL INFORMATION THAT CAN BE SUBJECT TO CHANGE AND ALTERATION, FOR CRIMINAL AND ILLEGAL INDOLE.

INTRODUCCION

Con el rápido avance de la tecnología en los últimos años cada vez a pasos más acelerados y el acceso al Internet en casi todo el planeta, sin lugar a dudas que el mundo se ha digitalizado. Desde los aspectos más humanos y sensibles como la música o el cine, hasta los más especializados procesos y actividades desarrolladas por el hombre, como son las complejas transacciones financieras que hoy en día atraviesan el mundo en fracciones de segundo se manejan hoy a través de computadores y redes globales.

Pero nada es perfecto, con el rápido avance de la tecnología, también se invento una nueva forma de delito, rápida y muy eficaz como el avance de la tecnología, es así que los **DELITOS INFORMATICOS** en la actualidad es una nueva forma de realizar actos ilícitos por parte de las personas que saben de los mismos.

Pues para cometer este tipo de delitos normalmente es necesario el conocimiento de la informática, aunque algunos de los mismos no son tan difíciles de realizar.

Pese a que la Ley de Comercio Electrónico recoge algunas disposiciones sobre el manejo de información electrónica, en el Ecuador los delitos informáticos no están tipificados ni sancionados en el Código Penal.

Esto debido a que en el país son cada vez más comunes los fraudes informáticos, suplantación de identidad por internet o por teléfono, y los 'troyanos bancarios' que se instalan en diferentes aparatos simulando ser otro tipo de programas para obtener información de entidades financieras.

Empresas de toda índole y a nivel Mundial han sido perjudicadas por esta clase de delitos que a menudo son personas que están inmersas en el campo de la informática y con elevadas posibilidades de que no lleguen a descubrirles. Por

lo tanto, se trata de una delincuencia de especialistas capaces muchas veces de borrar toda huella de los hechos.

Del universo de varias decenas de millones de computadoras interconectadas, no es difícil pensar que puede haber mas de alguien con perversas intenciones respecto a nuestra organización, es por esta razón, que debemos tener nuestra red protegida adecuadamente, para no ser tal vulnerables a los ataques informáticos de personas inescrupulosas..

A principios de la década de 1980, los tribunales de varios países desarrollados enfrentaron los primeros problemas que surgieron por desiciones legislativas que reconocieron a los programas de computación como un elemento que podría ser protegido y usado como un medio mas para el comedimiento de delitos.

El derecho informático podría definirse como el conjunto de normas y preceptos que regulan el uso de la tecnología informática por parte de las personas, empresas e instituciones.

Se trata de una rama del derecho privado muy joven, pero con un campo de acción muy amplio, debido a que la tecnología informática ha invadido todos los aspectos de las personas, desde su intimidad mas secreta hasta sus relaciones con la familia, la religión, la educaron de sus hijos, los amigos, las empresas, el medio ambiente y el mundo exterior.

CONCEPTO DE DELITO INFORMATICO

Encontramos tantos conceptos del mismo, cuantos investigadores del tema existen citare algunos de ellos: **Nidia Callegari,** define el delito Informático como "aquel que se da con la ayuda de la informática o de técnicas anexas".

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

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

Por lo tanto, resumiendo, diremos que Delitos Informáticos son aquellas conductas ilícitas susceptibles de ser sancionadas por el Derecho Penal, que hacen uso indebido de cualquier medio informático.

TIPOS DE DELITOS

Brevemente analizaremos alguno de los delitos informáticos más comunes, los mismos que se desarrollan de manera habitual por quienes realizan estas actividades ilícitas.

EL PHARMING y EL PHISHING

Consisten en el robo de su información personal a través de señuelos para que usted ingrese su información, páginas web falsas, correos electrónicos que parecen provenir de su institución financiera o de empresas con las que usted tiene algún tipo de relación.

De apariencia muy similar a las originales, obtienen sus datos a través de un correo electrónico supuestamente en blanco o de la misma página falsa que termina robando sus datos, haciéndole creer que debe enviar sus claves o datos tales como su nombre, numero de cédula, número de cuenta o número de tarjeta, dirección, teléfono, etc. para asuntos de confirmación o actualizaciones, transferencias o premios de los que supuestamente usted es el acreedor.

EL SKIMMING y EL SCANNING

En estos tipos de fraude como sus nombres indican, el delincuente copia o escanea la información financiera y personal de su tarjeta de crédito o débito y luego la regraba en una tarjeta falsa, creando así una replica que tiene los mismos alcances y limitaciones que su tarjeta personal. Para llevar a cabo el fraude el delincuente utiliza un pequeño aparato que se instala en la ranura del cajero automático y que al momento de que usted inserta su tarjeta, copia inmediatamente su información, mientras un compinche o el mismo estafador, se posiciona de tal manera para poder percatarse de los números de su clave y así al momento que usted abandona el cajero de su entidad, el criminal retira sus fondos con la tarjeta clonada.

LAS REDES SOCIALES

Las muy populares redes sociales, como son Hi5, Facebook, MySpace y muchas otras más, extendidas por todo el mundo de amigo a amigo, o de conocido a conocido, son preferidas por los estafadores para acceder fácilmente a su información personal y se usan también como puertas de entrada inyectando pequeños programas que ingresan en su sistema copiando su información personal para fines delictivos.

Usualmente el estafador envía un mail que se supone proviene de la red social de su preferencia y que al momento de abrir, roba su información personal, o simplemente el delincuente se crea varias personalidades virtuales con el propósito de captar amigos y así ingresar en sus perfiles y enterarse de sus modos de vida, de trabajo, de sus horarios y así aprovechar las ventajas

que ofrece el usuario al publicar su información sin ninguna precaución y, al enterarse de los detalles de la vida de su víctima, el hábil estafador incluso puede programar un asalto a su casa o negocio sin que usted pueda hacer nada, ya que por ejemplo en esos momentos usted está trabajando o está de vacaciones.

EL SNIFFING

Es un método en el cual los delincuentes roban información de un terminal específico o de una red, instalando un apartado o un cable que cumple las funciones de un espía, grabando todo lo que entra y sale del terminal con la finalidad de conseguir sus claves, intervenir en su correo electrónico, en su página de chat, etc.

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

Qué son los gusanos:

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

Qué es la bomba lógica o cronológica:

Es aquella que exige conocimientos especializados, ya que requiere la programación de la destrucción o modificación de datos.

Es importante destacar, que a diferencia de los virus o gusanos, las bombas lógicas son difíciles de detectar antes de que exploten; es por esta razón, que de todos los dispositivos informáticos criminales, la bomba lógica es la que más daño hace dentro del sistema informático.

Es difícil saber cuál es el sujeto, por cuanto se puede programar la detonación para que tenga lugar mucho tiempo después de que se haya marchado el criminal informático.

Es muy importante diferenciar entre el Hacking y Cracking, el primero, utiliza técnicas de penetración no programadas para acceder a un sistema informático, buscando únicamente el ingreso a tales sistemas sin dirigir sus

actos a la afectación de la integridad o disponibilidad de la información, pero sí a la confidencialidad y exclusividad de la misma y también en algunos casos a vulnerar la intimidad del titular de aquella; mientras que el segundo, altera, suprime o daña la información, por cuanto la intención del agente es obstaculizar, dejar inoperante o menoscabar el funcionamiento de un sistema o dato informático.

LOS SUJETOS EN EL DELITO.

SUJETO ACTIVO

En este tipo de delitos, el sujeto activo debe tener conocimientos técnicos de informática, es decir, en cierto modo, una persona con nivel de instrucción elevado, para poder manipular información o sistemas de computadora.

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

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

SUJETO PASIVO

En el caso del Delito informático pueden ser. Individuos, instituciones de crédito, gobiernos, en fin entidades que usan sistemas automatizados de información.

En primer termino tenemos que distinguir que el sujeto pasivo o victima del delito, es el ente sobre el cual recae la conducta de la acción u omisión que realiza el sujeto activo, y en el caso de los delitos informáticos, mediante el

podemos conocer los diferentes ilícitos que cometen los delincuentes informáticos, que generalmente son descubiertos casuísticamente debido al desconocimiento del modus operandi.

Ha sido imposible conocer la verdadera magnitud de los Delitos Informáticos, ya que la mayor parte de los delitos no son descubiertos o no son denunciados a las autoridades responsables; que sumado al temor de las empresas de denunciar este tipo de ilícitos por el despresgio y su consecuente perdida económica que esto pudiera ocasionar, hace que este tipo de conductas se mantengan bajo la llamada "cifra oculta" o "cifra negra".

DELITOS INFORMATICOS EN EL ECUADOR

A partir de la década de los sesenta, la humanidad descubrió las ventajas que trae consigo la tecnología.

El ser humano poco a poco, logro automatizar muchas de sus actividades, se ahorra tiempo y recursos con el empleo de lo que se denomina "inteligencia artificial" es difícil imaginar alguna actividad humana en la que no intervengan maquinas dotadas de gran poder de resolución.

La informática entendiéndola como el uso de computadoras y sistemas que ayudan a mejorar las condiciones de vida del hombre, la encontramos en todos los campos: la medicina, en las finanzas, en Derecho, en la industria, entre otras. En la actualidad con la denominada "autopsia de la información", el Internet, las posibilidades de comunicación e investigación se han acrecentado, se tiene acceso a un ilimitado número de fuentes de consulta y entretenimiento.

El problema radica en que la conducta humana parece ser que esta inclinada al delito, a conseguir satisfacción de sus deseos a toda costa, con el desarrollo de la informática, aparece también lo que se denomina, el **DELITO INFORMÁTICO.**

De la misma manera que muchas personas sean dedicado a desarrollar sistemas de computación para solucionar problemas de la sociedad, otras

tratan de utilizar la tecnología, y en el caso que nos ocupa, las computadoras y sistemas para el cumplimiento de sus actividades ilícitas.

Es oportuno indicar, que legislaciones a nivel mundialhan tipificado como delito esta clase de actividad y la han sometido a sanciones penales. En el Ecuador, nuestro Código Penal tipifica a este delito como "Daño Informático", imponiendo una prisión de 6 meses a 3 años y multa de 60 a 150 dólares para aquél que en forma maliciosa, destruya, altere, suprima o inutilice programas, bases de datos o sistema de redes o sus partes, o impida, obstaculice o modifique su funcionamiento. Se agrava la pena de 3 a 5 años y multa de 200 a 600 Dólares en caso de que afectare datos contenidos en la computadoras o en el sistema de redes destinado a prestar un servicio público oque tengan que ver con la Defensa Nacional.

El sabotaje informático, es llevado a cabo, en la mayoría de los casos por empleados descontentos y puede producirse, tanto a la parte física del ordenador (hardware) como a la parte lógica del mismo (software). Los daños al software se pueden causar a través de elementos electromagnéticos, cuyas técnicas son las siguientes: la introducción de virus, gusanos o una bomba lógica que destruye, altere o inutilice los programas, datos o documentos electrónicos almacenados en el sistema informático.

El ART. 202. 1. [Utilización de medios electrónicos para violar claves, sistemas de seguridad o acceder a información protegida]. "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 reprimida 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 serpa de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica.

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

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

El tratadista Ignacio Carvajal Remires diferencia lo que se ha de entender por Derecho Informático e Información Jurídica en los siguientes términos: el Derecho Informático es una rama de la ciencia jurídica que considera a la informática como un instrumento y también como objeto de estudio.

La Informática Jurídica resulta así del conjunto de aplicaciones de la informática y el derecho, generando de esta manera normas y principios aplicables a los hechos y actos derivados de la informática (Fuente de Información: Jurismática).

El mundo globalizado exige respeto a las creaciones intelectuales, los bienes intangibles han cobrado su real importancia con el devenir del tiempo y hoy su validez es igual o mayor que la de los bienes tangibles, por tato su adecuada protección es vital para el desarrollo tecnológico y económico de los países.

El sofware o programas de ordenador, son obras intelectuales sui generis que requieren una protección específica, ya que constituye el resultado de un esfuerzo creativo, de inversión de tiempo y dinero.

La adquisición de un programa de ordenador a su propietario a de realizar única y exclusivamente:

a) Una copia del programa con fines de seguridad.

b) Fijar el programa en la memoria interna del aparato, para su utilización.

c) El uso normal previsto en la licencia.

Para cualquier otra utilización inclusive la reproducción para fines de uso personal o el aprovechamiento del programa por varias personas a través de redes u otros sistemas análogos, se requiere de la autorización del titular de los derechos, autorización que se traduce por lo general en una licencia de uso.

En los últimos años, la seguridad informática a nivel mundial ha sido vulnerada por el aumento de personas inescrupulosas, que con el fin de acceder a un sistema violan medidas de seguridad, poniendo en peligro, la integridad, confidencialidad o disponibilidad de los sistemas informáticos y de los datos almacenados en ellos.

El Artículo 202. 1 contempla la pena de seis meses a un año de prisión y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica a quien, "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".

El Inc. 2° del propio artículo, considera una figura agravada, imponiendo una pena de uno a tres años de prisión y multa de mil a mil quinientos dólares de los Estados Unidos de Norteamérica, si la información obtenida se refiere a la "seguridad nacional o secretos comerciales o industriales".

PHIL WILLIAMS Profesor de Estudios de Seguridad Internacional, Universidad de Pittsbugh nos dice que es necesario contar no solo con leyes e instrumentos eficaces y compatibles que permitan una cooperación idónea entre los estados para luchar contra la Delincuencia Informática, sino también con la infraestructura tanto técnica como con el recurso humano calificado para hacerle frente a este nuevo tipo de delitos.

La tecnología de las comunicaciones también confiere más flexibilidad y dinamismo a las organizaciones delictivas; el correo electrónico se ha convertido en un instrumento de comunicación esencial independiente del tiempo y la distancia.

Las autoridades encargadas de hacer cumplir la ley suelen adaptarse con lentitud a las nuevas tendencias, mientras que los grupos delictivos organizados tienden a adaptarse rápidamente y a aprovechar los adelantos tecnológicos debido a los inmensos beneficios que producen sus actividades ilícitas.

La apertura de nuevos mercados y las nuevas tecnologías de las comunicaciones, junto con la diversidad de actividades en las que participan, también han alimentado el crecimiento de la delincuencia organizada en los países en desarrollo. Los países con economías en transición o en situaciones de conflicto son particularmente vulnerables al crecimiento de ese tipo de delincuencia. En tales casos, la delincuencia organizada plantea una amenaza real para el desarrollo de instituciones reformadas, como la policía, los servicios de aduana y el poder judicial, que pueden adoptar prácticas delictivas y corruptas, planteando un grave obstáculo al logro de sociedades estables y más prósperas.

La delincuencia organizada y las prácticas corruptas van de la mano: la corrupción facilita las actividades ilícitas y dificulta las intervenciones de los organismos encargados de hacer cumplir la ley.

La lucha contra la corrupción es, por lo tanto, esencial para combatir la delincuencia organizada. Es más, se ha establecido un nexo entre la delincuencia organizada, la corrupción y el terrorismo. Algunos grupos terroristas, por ejemplo, han recurrido a la delincuencia organizada para financiar sus actividades.

Por consiguiente, la promulgación de legislación apropiada, el fomento de la capacidad de hacer cumplir la ley y la promoción de la cooperación internacional para luchar contra las actividades de la delincuencia organizada y las prácticas corruptas conexas también fortalecen la capacidad de combatir el terrorismo.

En nuestro País, en abril de 2002, expide la Ley de Comercio, Firmas Electrónicas y Mensajes de Datos, instrumento que da un marco jurídico a las innovaciones tecnológicas relacionadas con la transmisión de información utilizando medios electrónicos.

El objeto de la Ley es la de regular los mensajes de datos, firmas electrónicas, servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos a través de redes de información, incluido el comercio electrónico (e-business) y lógicamente la protección a los usuarios de estos sistemas de cualquier mecanismo de distorsión.

Gracias a la expedición de esta Ley, nacen como delitos con características propias el sabotaje (SPAM) y los daños informáticos (CYBER CRIME). Sobre este punto trataremos más adelante, hasta mientras diremos que estas infracciones se incorporan al Código Penal ecuatoriano, logrando así una protección concreta y específica a este tipo de actos, considerados desde abril de 2002 como delitos.

Ahora bien, dentro de la regulación propia de los mensajes de datos, también se prevé mecanismos de protección propios en donde se enuncian principios y procedimientos que se deben respetar.

El artículo 5 de la Ley establece principios sobre confidencialidad y reserva: "se establecen los principios de confidencialidad y reserva para los mensajes de datos, cualquiera sea su forma, medio o intención.

Toda violación a estos principios, principalmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional, será sancionada conforme a lo dispuesto en esta Ley y demás normas que rigen la materia". Se establecen principios

Con relación a la protección de datos, para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información que quiera compartir con terceros.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato".

La norma protege a la elaboración, transferencia o utilización de bases de datos, siempre enmarcada dentro de principios de confidencialidad y privacidad. En cualquiera de estos casos, es un requisito sine qua non el consentimiento del titular, pero no será necesario este consentimiento expreso cuando se trate de situaciones que generen correspondencia entre las partes para crear una base de datos.

Resumiendo, vemos que existen principios constitucionales y legales de protección a la información que consta en una base de datos. Los mensajes que se generen, deben estar acompañados siempre de criterios y parámetros de respeto al bien ajeno y a la propiedad privada.

Por esto se requiere el consentimiento para que sea posible disponer del mensaje recibido o sujeto de envío. También es importante resaltar que se prohíben las bases de datos y la recopilación de direcciones electrónicas, salvo que exista un consentimiento por parte del dueño o sea producto de funciones propias que se desempeñen entre partes y que se vayan generando con el transcurso del tiempo.

La Ley considera que si se recopila y usan datos personales sin el consentimiento previo, existe una violación flagrante a los derechos de la privacidad, confidencialidad e intimidad que se encuentran garantizados por la Constitución.

El campo de aplicación de la Ley de Comercio y Firmas Electrónicas está dado básicamente por relaciones contractuales amparadas en el campo civil, aunque también, de menor manera, tiene injerencia dentro del ámbito penal.

Este ámbito está dado concretamente dentro de lo que ésta misma considera como infracciones informáticas. La Ley agregó al Código Penal una serie de infracciones antes no contempladas para sancionar este tipo de delitos.

"Falsificación electrónica: son reos de falsificación electrónica la persona o personas que con el ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio, **ALTEREN O MODIFIQUEN MENSAJES DE DATOS, O LA INFORMACIÓN INCLUIDA EN ÉSTOS**, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

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

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

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

Para tener una idea sobre la ubicación de la norma dentro del Código Penal, el legislador ha considerado que estos delitos se deben encasillar dentro de los delitos contra la propiedad y concretamente dentro del delito de robo.

Esta disposición protege al consumidor de cualquier tipo de información que sea falsa. Cuando se refiere a información comercial que induzca a error o engaño, la Ley de Defensa del Consumidor establece protecciones y sanciones para evitar que este tipo de prácticas se generalicen, lógicamente, protegiendo al consumidor para que no se le oferte un producto de una calidad y reciba otra de distinta a la ofertada.

La Ley de Defensa del Consumidor no establece de manera expresa una protección al consumidor, pero si de manera general, principios de aplicación que se pueden aplicar para este caso en concreto.

Hay otra disposición que no deja de ser interesante. Dentro de los nuevos artículos que se incorporan al Código Penal ecuatoriano consta el siguiente:

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

EstE artículo establece como delito a la recolección indiscriminada de cuentas de emails y la prohibición de ventas o comercialización no autorizada de cuentas de mail, para fines netamente comerciales.

Sobre el envío de comerciales no solicitados o que en los mensajes, cuando se envía propaganda, se establezca alguna señal (ADV en Estados Unidos), no hay una regulación específica sobre el tema, por lo que consideraría que no hay limitación ni regulación alguna que obligue a especificar a quien envía que el mensaje contiene propaganda. La única limitación que puede existir es el respeto hacia terceros y principios constitucionales que garanticen un respeto al consumidor, pero ni siquiera así, ya que me parece muy difuso si no existe una norma concreta al respecto.

De esta manera se ha hecho un amplio esbozo sobre la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y la manera como la legislación ecuatoriana protege este tipo de actos dándoles la categoría de delitos.

De todos modos, quiero repasar puntualmente ciertas preguntas que son usualmente formuladas, con el fin de que estos temas sean resueltos de la manera más clara posible:

"Si podemos usar otras normas para atacar el envío de spam, como por ejemplo, leyes de protección de consumidores o sobre privacidad"

Si bien la Ley de Defensa del Consumidor establece normas generales sobre inducir a error o engaño relacionado con propagando o difusión de información, la ley compete en estos casos, por ser una ley específica sobre la materia, va a

ser la Ley de Comercio Electrónico. Como vimos anteriormente, el SPAM está regulado por la Ley de la materia.

"Hay leyes sobre spam o emails que traten con temas particulares como pornografía, distribución de un virus u otro código malicioso, u oferta de bienes ilegales"

Dentro de la Ley de Comercio Electrónico, sobre distribución de virus u otro código malicioso, se regulan dentro de las disposiciones ya analizadas. En el caso de pornografía u oferta de bienes ilegales, no existe ninguna prohibición ni norma al respecto relacionada directamente con la difusión a través de medios electrónicas de manera específica, pero en el Código Penal de manera más amplia, dentro de los delitos sexuales, considera como un atentado contra el pudor a este tipo de manifestaciones, sin importar el medio que se utilice.

La ley se expidió recientemente, por lo que no hay ningún fallo jurisprudencial o doctrina que avalen este criterio.

Sin embargo, hay normas constitucionales que protegen la honra, la moral, las buenas costumbres, la libertad, la falta al decoro y la dignidad personal, que se ven alterados con el envío de este tipo de información.

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

La cooperación multilateral de los grupos especiales multinacionales pueden resultar ser particularmente útiles - y ya hay casos en que la cooperación internacional ha sido muy efectiva. De hecho, la cooperación puede engendrar emulación y éxitos adicionales.

De otro lado en los últimos tiempos la masificación de virus informáticos globales, la difusión de la pornografía infantil e incluso actividades terroristas son algunos ejemplos de los nuevos delitos informáticos y sin fronteras que presentan una realidad difícil de controlar.

Con el avance de la tecnología digital en los últimos años, ha surgido una nueva generación de delincuentes que expone a los gobiernos, las empresas y los individuos a estos peligros.
Es necesario también hacer mención a la **Convención Internacional sobre el Cibercrimen del Consejo de Europa.**

Esta Convención busca como objetivos fundamentales los siguientes:

1. Armonizar las leyes penales sustantivas aplicables a las conductas delictivas que tienen como escenario el entorno informático;

2. Proveer reglas de procedimiento penal que brinden a las autoridades nacionales competentes las facultades necesarias para la investigación y persecución de tales conductas delictivas; y

3. Establecer un régimen dinámico y efectivo de cooperación internacional.

Haciendo un breve estudio de los acontecimientos recientes, muestra que en la mayoría de países existe una ambigüedad acerca de la protección de posdelitos informáticos, situación que debe ser resuelta por medio de una clarificación legal.

Algunas autoridades y tribunales se han mostrado prudentes en declarar hasta que punto las innovaciones informáticas tienen la posibilidad de ser registradas,

El Sabotaje informático doctrinariamente, es el acto de borrar, suprimir o modificar sin autorización funciones o datos del sistema informático (hardware y/o software) con intención de obstaculizar el funcionamiento normal del sistema.

Es acceder sin ser autorizados a servicios y sistemas informáticos que van desde la simple curiosidad, como es el caso de los piratas informáticos (hackers), hasta el sabotaje informático (ckacking).

Este delito, puede entrañar una perdida económica sustancial para los propietarios legítimos de Empresas, Instituciones públicas, privadas, Gubernamentales, etc.

El Sabotaje o Daño Informático puede tener lugar en Internet en dos formas:

a) Puede producirse por medio de la modificación y/o destrucción de los datos o programas del sistema infectado.

b) puede producirse por medio de la paralización o bloqueo del sistema, sin que necesariamente se produzca alteración ni destrucción de los datos o programas.

Desde el punto de vista jurídico no es aceptable que el software, que ha sido desarrollado mediante un esfuerzo intelectual e inversiones que en ocasiones resultan cuantiosas, pueda ser aprehendido y ilegítimamente, es decir, que se apodere de él sin derecho, y sin autorización de las personas que pueden disponer de dichos programas con arreglo a la ley.

Sin embargo el problema de la protección jurídica del software no es de solución sencilla. Como se ha señalado con relación a que en los conocimientos técnicos, el derecho no puede admitir ni tolerar el apoderamiento de los mismos.

Pero tampoco debe, proteger exageradamente los derechos de los inventores, de tal suerte que su ejercicio perjudique a la sociedad, ni favorecer el desequilibrio tecnológico existente entre países con diverso grado de desarrollo, al otorgar monopolios que solo contribuyen a beneficiar a los países industrializados.

Se debe considerar que se debe propiciar laceración de un verdadero derecho informático, dentro del ámbito inclusive del derecho económico, como una rama especial de la ciencia jurídica, basada en los principios de la Propiedad

Intelectual, y acorde con las nuevas exigencias de la tecnología y con la evolución de la industria y comercio que es la aspiración de los países del continente americano.

Es obvio que las normas del derecho informático deben ajustarse alas realidades que impone la actual situación del mundo, pero al estar reglados por la justicia, como una consideración de superior axiología, sin duda contribuirán al bienestar del hombre, que es el objetivo último del derecho.

Formalmente la manera mas simple de proteger las creaciones intelectuales es la de hacer valer en poscontratos de prestación su carácter secreto.

Es necesario agregar lo que el profesor alemán Klaus Tiedemann afirmará "la criminalidad informática representa un ejemplo y una justificación actualizada de la siguiente afirmación: una legislación (penal) que no tome en cuenta prácticas ya realizadas o conocidas en otros Estados en y con computadoras estaría desde un comienzo condenada al fracaso y una discusión internacional amplia que compare las diferentes experiencias para acabar con la criminalidad de computadoras sería con justicia la indicada para conseguir este objetivo."

Ante la necesidad de proteger a los usuarios de la red frente a la emergente criminalidad informática, que aprovecha las vulnerabilidades de los sistemas informáticos y el desconocimiento generalizado de la mayoría de los usuarios de la cultura digital, y ante la perentoria obligación de extender especialmente tal protección a los menores, que sufren una mayor indefensión y son víctimas de delitos como el de la pornografía infantil, sobre todo en las zonas más deprimidas y menos desarrolladas del planeta.

Esto tomando en cuenta que las nuevas tecnologías aportan una indiscutible mejora en la calidad de vida de nuestra sociedad. Por ello, han de promoverse cuantas iniciativas sean posibles para el desarrollo de la sociedad de la Información y su buen uso, a la vez que garantizar la seguridad de sus usuarios, y así poder terminar con la llamada **Cifra Negra**, en esta clase de infracciones.

El desarrollo tan amplio de las tecnologías informáticas ofrece un aspecto negativo, el mismo ha abierto la puerta a conductas antisociales y delictivas que se manifiestan de formas que hasta ahora no era posible imaginar.

Es deber del Estado y en especial de la Fiscalía el de promover las dinámicas sociales, jurídicas, tecnológicas, policiales, o de cualquier otra índole para hacer frente de forma eficaz al problema de la delincuencia informática.

De igual forma el Estado debe velar porque las aplicaciones de la tecnología sean correctas en el marco de la legalidad y de la ética, partiendo de bases y principios comunes que sean aceptados por la comunidad global, única manera de tener y mantener una verdadera protección al derecho a la intimidad.

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

Como ya lo habíamos manifestado anteriormente sin duda alguna el avance que trajo consigo el Internet, ha hecho también que la pornografía, incluso infantil sea mas vista y practicada en la actualidad, pues no es raro que existan muchas paginas el la red que oferten imágenes, videos y hasta servicios de mujeres menores.

Lo que sin duda alguna debería de ser controlado por las autoridades de nuestro país con el fin de evitar que estas prácticas se proliferen y continúen en nuestra sociedad.

Para mi punto de vista si bien nuestro Código Penal tipifica ciertos delitos informáticos, estos deberían de tener un tratamiento especial, tipificar los mismos en su totalidad, y no solo eso si no que se debería de tener en cuenta

que día a día van naciendo nuevas formas de cometer delitos, por lo que se debe de crear la policía especializada en delitos informáticos en nuestro país.

Ahora si bien las tendencias actuales buscan un aceleramiento de sus operaciones, tal es el caso de las Instituciones bancarias, debemos de tener muy en cuenta con que facilidad pueden los individuas que se dedican al fraude informatico, pueden tener acceso a la información de los clientes, y tener también muy en cuenta la seguridad de los medios por los cuales se realizan las transacciones y negocios de las mismas.

Una solución sin duda alguna seria regular de mejor manera los delitos informáticos existentes, tipificar cada una de estos y establecer sanciones para los infractores, pero sin duda alguna esto se lo debe realizar con el apoyo de las entidades que administran justicia en nuestro país, para que se de la creación de una ley propia de delitos informáticos.

En síntesis, es importante poner de relieve que la delincuencia cibernética, generalmente se basa en el delito instrumentado por el uso de la computadora a través de redes telemáticas y la interconexión de la computadora. Las ventajas y las necesidades del flujo nacional e internacional de datos, que aumenta de modo creciente en Países donde la tecnología está más avanzada y en otros donde se está desarrollando notablemente, conlleva también a la posibilidad creciente de estos delitos.

BIBLIOGAFIA

- **CODIGO PENAL.**
- **LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS**. (Ley No. 2002-67).
- **CARVAJAR RAMIREZ IGNACIO,** INFORMATICA JURÍDICA.
- **WILLIAMS PHIL,** Crimen Organizado y Cibernét ico, sinergias, tendencias y respuestas. Centro de Enseñanza en Seguridad de la Internet de la Universidad Carnegie Mellon.
- **RINCON CARDENAS, Erick**. Manual de Derecho y Comercio Electrónico en Internet.