PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE JURISPRUDENCIA

ESCUELA DE DERECHO

DISERTACION PREVIA A LA OBTENCIÓN DEL TÍTULO DE

ABOGADO DE LOS JUZGADOS Y TRIBUNALES DE LA REPÚBLICA DEL ECUADOR

"EL DELITO INFORMÁTICO: SU EVOLUCIÓN, PUNIBILIDAD Y PROCESO PENAL EN EL ECUADOR"

HUGO ALEXANDER CUENCA ESPINOSA

DIRECTOR: DR.SANTIAGO ACURIO DEL PINO

QUITO, 2014

CERTIFICADO DE APROBACIÓN DE TESIS

En mi calidad de Director de Tesis de la carrera de Derecho, de la Facultad de Jurisprudencia de la Pontificia Universidad Católica del Ecuador.

CERTIFICO:

Que, luego de la correspondiente revisión y análisis, apruebo en su totalidad el Trabajo de Tesis de Grado presentado por el Sr. Hugo Alexander Cuenca Espinosa, como requisito previo para acceder al grado académico de "ABOGADO DE LOS JUZGADOS Y TRIBUNALES DE LA REPÚBLICA DEL ECUADOR".

El tema de la investigación se refiere a: **"EL DELITO INFORMÁTICO: SU EVOLUCIÓN, PUNIBILIDAD Y PROCESO PENAL EN EL ECUADOR"**.

Quito, Mayo del 2014

……..

Dr. Santiago Acurio del Pino

DIRECTOR DE TESIS

DECLARACIÓN DE AUTORÍA Y ORIGINALIDAD

Por la presente, declaro bajo la solemnidad de juramento, que soy el único Autor de la Tesis **"EL DELITO INFORMÁTICO: SU EVOLUCIÓN, PUNIBILIDAD Y PROCESO PENAL EN EL ECUADOR"**, que presento como requisito previo para acceder al grado académico de ABOGADO.

La tesis es original en su formulación conceptual, procedimientos de investigación, desarrollo del aparato demostrativo, análisis de los resultados y conclusiones, a excepción de referencias, conceptos, procedimientos, datos o afirmaciones provenientes de otros trabajos, en cuyo caso han sido citados en forma textual o implícita, según el caso.

Declaro además que este trabajo no ha sido previamente presentado en ninguna otra institución educativa, u organización pública o privada, ni lo será, sin hacer expresa mención a su condición de tesis presentada por mí y bajo mi autoría, en esta Institución.

Quito, Mayo del 2014

……..

Sr. Hugo Alexander Cuenca Espinosa

C.C. 172104755-1

“Pienso que los virus informáticos muestran la naturaleza humana: la única forma de vida que hemos creado hasta el momento es puramente destructiva”

– Stephen Hawking

“Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnología”

– Bruce Schneier

DEDICATORIA

A mis padres Hugo y Cecilia, quienes depositaron su confianza, sacrificio y esfuerzo en mí para que yo pudiese cumplir mis sueños, deseos y metas y, por darme la mano cuando sentía que el camino se estrechaba, a ustedes mi cariño, afecto y gratitud.

A mis abuelos Enrique y María, y a mi tía María Elizabeth a quienes debo mis valores y costumbres, sobre todo por la crianza en mis primeros años de vida, agradecimiento eterno hacia ustedes.

A mi hermano Bryan Steven, legado de mi sangre, por su paciencia y comprensión.

A mis primos Fabricio y Darwin, por su apoyo y lealtad, gracias por lo momentos compartidos.

A mis familiares, amigos y conocidos que han sido motivo de inspiración, además de brindarme palabras de aliento, éxito y suerte en los momentos altos y bajos de mi vida.

AGRADECIMIENTO

A mis maestros Dr. Adrián Corvalán Liquitay, Dr. Hernán Salgado Pesantes, Dr. Guillermo Enríquez, Dra. Paulina Araujo Granda, Dr. Santiago Guarderas Izquierdo, y al Padre Dr. Efrén Vivar, que en este andar por la vida, influyeron con sus lecciones y experiencias en mi construcción profesional, además de haberme brindado su amistad, respaldo y guía al momento de plantear inquietudes académicas y profesionales que me ayudaron a mejorar íntegramente como ser humano y ahora como abogado para asumir cada uno de los retos que impone la sociedad, a todos ellos les dedico cada una de estas páginas, en especial a mi Director de Tesis y amigo Doctor Santiago Acurio del Pino, quien con su amistad y apoyo ha logrado guiarme por esta nueva rama del Derecho, dando esas pautas primordiales para ser un abogado de éxito en la materia penal informática, muchas gracias por lo compartido maestro.

RESUMEN O ABSTRACT

Con el avance de la tecnología y el aumento de las vías de comunicación, han ido incrementando las formas de delinquir, dando paso a nuevos modos para la consumación de delitos, es así que los delitos tradicionales aunque no obsoletos han quedado un tanto en el pasado. En la actualidad la consumación de los delitos ya no se los da sólo de forma típica conocida también como clásica o tradicional, sino a través de medios informáticos y electrónicos, en lo que llamamos generalmente "Delitos Informáticos", delitos que en principio resultan difíciles para la compresión de Abogados, Fiscales y Jueces, puesto que para su entendimiento no sólo se necesita de un conocimiento legal sino también técnico.

La presente tesis en principio nació como un trabajo de investigación académico en relación al Fenómeno del Cibercrimen realizado en el año 2009 mientras cursaba mis estudios superiores en la Facultad de Jurisprudencia de la Pontificia Universidad Católica del Ecuador, para aquel entonces el tema ya conocido en otros países, pero aun nuevo en el Ecuador, comenzaba a ser controversial por los primeros ataques y blancos de delitos informáticos. Lo que comenzó como un proyecto universitario pasó hacia objetivos mayores por lo amplio, variado, novedoso e interesante que puede resultar este tema, inclusive porque se lo considera más un "fenómeno" que "delito", puesto que contiene una variedad de caracteres Criminológicos y Forenses como la escena del delito, psicología criminal, y otros, que lo convierten en un tema de amplio estudio, donde puedo destacar el análisis de la conducta criminal del ciberdelincuente hasta el desenvolvimiento del mismo para la comisión del delito.

Debo reconocer que parte del presente trabajo lo logré con la ayuda y guía de varias personas que a lo largo, no solo de la investigación, sino de la vida me ayudaron a tener esa variedad de experiencias que me sirvieron como aporte fundamental para entender, comprender, analizar, y juzgar este fenómeno desde diferentes puntos; esta serie de experiencias variaron desde el conocer el Hacking puro en el Underground (bajo mundo del Hacking) hasta el Hacking Ético para utilizarlo como herramienta de bienestar social con apego a la ley, y a través de mi experiencia como Analista de Inteligencia en la Dirección Nacional de Investigaciones de la Fiscalía General del Estado, y posteriormente

como Investigador y Analista en la Secretaria Nacional de Inteligencia. Otro motivo fue los continuos cambios que sufre este fenómeno por las nuevas técnicas, usos y modalidades, pues como se sabe la tecnología está en constante evolución; esta motivación a su vez nació de mi relación con nuevos participes involucrados en el tema de la lucha contra el Cibercrimen y su investigación, no sólo en Ecuador sino a nivel internacional, pues un aporte fundamental fue el compartir experiencias, vivencias y anécdotas con agentes y analistas de inteligencia de la CIA, DAS, DGI, Interpol, además de Abogados, Hackers y Especialistas en el tema de países de habla hispana e inglesa en diferentes eventos y reuniones en los que he sido partícipe dentro y fuera del Ecuador.

Como ya lo he mencionado anteriormente el fenómeno del Cibercrimen es cambiante o evoluciona, pues a diario surgen nuevas modalidades para la comisión de ilícitos, a su vez causa un impacto en el sector económico, social y político, por lo que hoy en día es motivo de controversia, ya que quién no ha escuchado de temas como Wikileaks, ciberespionaje, robo y suplantación de identidad, robo de dinero de cuentas bancarias, clonación de tarjetas de crédito hasta temas de la cotidianidad como hackeo y hurto de cuentas personales de correo y de redes sociales, que en principio violan derechos no sólo de ciudadanos sino también de países, atentando contra la privacidad de información de lo que bien pueda hacer un Estado en el libre ejercicio de sus garantías constitucionales.

La finalidad del presente trabajo es brindar con el material investigado una solución doctrinaria y legislativa al problema del Cibercrimen, ya que en el Ecuador al haber escasez en doctrina e investigación sobre este fenómeno y ciertos vacíos legales impide un desarrollo técnico-legislativo en materia penal informática, y un desconocimiento total o parcial del tema por parte de abogados, legisladores y funcionarios encargados de ejercer justicia dentro del territorio ecuatoriano.

Dentro de los temas incluidos en la presente tesis, hago hincapié en un tema fundamental e importante que suele ser motivo de confusión para los juristas que se adentran a esta nueva rama del derecho, que es la diferencia entre Delitos Informáticos y Delitos Computacionales o en anglosajón “Computer Crime Vs. Cybercrime”; la tesis también trata de temas como técnicas, usos y modalidades empleados por los cibercriminales, tipología de delitos, hasta el procedimiento penal para hacer punible esta clase de ilícitos.

Espero que los temas tratados en la presente tesis sean de interés e investigación por futuros lectores, además de trascendencia en interesados en el campo penal informático.

Alexander Cuenca Espinosa

San Francisco de Quito, Mayo 2014

ÍNDICE

ABREVIATURAS

ABA	Asociación de Abogados de Estados Unidos (American Bar Association)
AN	Asamblea Nacional
CC	Código Civil ecuatoriano
CE	Comisión Europea
CNUDMI	Comisión de las Naciones Unidas para el Derecho Mercantil Internacional
CNJ	Concejo Nacional de la Judicatura
CMSI	Cumbre Mundial sobre la Sociedad de la Información
CPC	Código de Procedimiento Civil ecuatoriano
CP	Código Penal
COIP	Código Orgánico Penal Integral
CPP	Código de Procedimiento Penal ecuatoriano
CRE	Constitución de la República de Ecuador
DGI	Dirección General de Inteligencia
FGE	Ministerio Público o Fiscalía General del Estado
G8	Grupo de las Ocho Naciones
ICANN	Internet Corporation for Assigned Names and Numbers
INT	Interpol
LCEFEMD	Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos
NU	Naciones Unidas
PACC	Comisión de la ABA sobre delitos contra la privacidad e informáticos (ABA Privacy & Computer Crime Committee)
PJ	Policía Judicial
SIN	Secretaria de Inteligencia
TIC	Tecnologías de la información y la comunicación
UIT	Unión Internacional de Telecomunicaciones

CAPITULO I

EL FENÓMENO DEL CIBERCRIMEN

1.1. Antecedentes

A partir de los años sesenta, la humanidad dio paso al descubrimiento y desarrollo de la tecnología; en principio no fue de acceso a todas las personas pues, su infraestructura física y su costo imposibilitaron que una persona cualesquiera tenga acceso a estas. Con el avance de la tecnología el ser humano logró automatizar tiempo y recursos con el empleo de la llamada AI (Inteligencia Artificial), es decir el imaginar una actividad sin la intervención de la persona, con máquinas desarrolladas de gran potencia y magnitud que hagan el trabajo físico e intelectual del hombre.

En la actualidad con la creación de la denominada "autopista de la información", el INTERNET, las posibilidades de comunicación e investigación se han incrementado, por lo que se tiene acceso a un ilimitado número de fuentes de consulta y entretenimiento desde casi cualquier lugar del mundo.

El problema de los Delitos Informáticos radica en que no todas las personas aprovechan este recurso, como es la tecnología de la forma más correcta, y abusan de esta para la comisión de actos maliciosos y de satisfacción personal, esto nos lleva a pensar y concluir bajo estudios realizados de psicología criminal, que la conducta de ciertas personas parece ser que está inclinada a la comisión de delitos, y a la satisfacción de sus pretensiones personales a toda costa; así mismo existen muchas personas que emplean la tecnología para el bienestar de la sociedad, otras se han dedicado al abuso de esta para la comisión de ilícitos informáticos, dando como resultado nuevas formas de delinquir distintas de las convencionales. Es así que con el desarrollo de la informática y con la idea de nuevas formas de delinquir aparecen los llamados DELITOS INFORMATICOS.

> *"El delito Informático implica actividades criminales que un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin*

embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho de estos actos para evitar la impunibilidad". [1]

En el Ecuador de los casos suscitados en cuanto a Delitos Informáticos, de Enero a Diciembre del 2010 se recibieron más de 866 denuncias en diferentes fiscalías del país por delitos tradicionales cometidos por y con mecanismos informáticos, de las cuales 697 fueron apropiación ilícita, 86 denuncias propiamente de delito informático como vulneración a páginas de servicio público, 82 a páginas de servicio privado y 1 por estafa utilizando medios informáticos.[2]

Cabe señalar que de acuerdo con un estudio realizado por la Unidad de Investigación de Cibercrimen de la Policía Judicial del Ecuador, los delitos informáticos crecieron en un 360% en 2010, en comparación con 2009, dejando una pérdida aproximada de un millón de dólares. Estas estadísticas guardan relación con los reportes de la Fiscalía General del Estado, que indican que sólo en los tres primeros meses del año 2011 se han denunciado 1.308 delitos informáticos. Entre enero y diciembre del 2011, esta cifra se incrementó considerablemente, llegándose a receptar 3.662 denuncias por este tipo de delitos.[3]

[4]

[1] LEVENE, Ricardo y CHIARAVALLORTI, Alicia. "Introducción a los Delitos Informáticos, tipos y legislación"
Internet: http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml
Acceso: 01/12/2013
[2] REVELO, Héctor. "Estadísticas 2010, Delitos Informáticos en el Ecuador."
Internet: http://www.abogados.ec/2011/02/estadisticas-2010-delitos-informaticos-en-ecuador/
Acceso: 02/05/2012
[3] Ídem
[4] Logo de la Unidad de Investigación del Cibercrimen de la Policía Judicial de Ecuador

Para el año 2012, el reporte de la Fiscalía General del Estado, refleja que dentro de los Delitos por Apropiación Ilícita por medios electrónicos se reportaron 2721 casos con mayor incidencia en Pichincha, Guayas y Santa Elena, de los cuales 17 tuvieron dictamen acusatorio y 11 dictamen absolutorio. En cuanto a Falsificación Electrónica el número bajo a 105 casos, esto se debió por los consejos de seguridad que dieron instituciones del Estado e instituciones de la banca privada a los ciudadanos para que se mantengan alerta para evitar cualquier nuevo modo de operar de los delincuentes.[5]

En cuanto al reporte de la Dirección de Gestión Procesal Penal de la Fiscalía General del Estado, de Enero a Diciembre del 2013 se produjo las siguientes cifras: Daños Informáticos al Servicio Privado (3), Daños Informáticos al Sector Público (1), Apropiación Ilícita por medios electrónicos (2114), Falsificación Electrónica (136), Suplantación de Identidad por medios informáticos (1704), se puede destacar que aunque la incidencia ha sido casi la misma, ha habido un aumento en la suplantación de identidad a través de medios informáticos, sobre todo en redes sociales como Facebook y Twitter.[6]

1.2. Problemática de los Delitos Informáticos

El problema principal se suscita con la aparición de la tecnología y nuevas formas de delinquir, lo que conlleva a una evolución tecnológica a la par de una línea cronológica de continuos nuevos "modus operandi", que en la era digital culminan en una variedad de ilícitos, entre estos los informáticos.

Otro de los problemas radica en el desconocimiento del tema por parte del legislador para poder tipificarlos, esto para su posterior incorporación y aplicación a través del Código Penal; así también por la falta de capacitación en el tema a los jueces para que estos a su vez puedan comprender, juzgar y aplicar la correspondiente sanción normativa por esta clase de ilícitos.

En relación a la tipificación, estos tipos penales tienen ciertos vacíos legales, puesto que hay desconocimiento parcial en materia de política criminal sobre

[5] FISCALÍA GENERAL DEL ESTADO DE ECUADOR, Dirección de Gestión Procesal Penal – SINAEP. "Reporte de Delitos Informáticos 2009 – 2013". Acceso: 05/03/14
[6] FISCALÍA GENERAL DEL ESTADO DE ECUADOR, Dirección de Gestión Procesal Penal – SINAEP. "Reporte de Delitos Informáticos 2009 – 2013". Acceso: 08/03/14

criminalidad informática; incluso si estuvieran bien tipificados, una errónea interpretación de la norma por parte de los jueces, puesto que esto también es técnico, llevaría a una inseguridad jurídica dando como resultado un agravio al accionante como al procesado, que puede reflejarse en un resultado no esperado para el accionante y/o una indebida aplicación del tipo penal para el procesado; esto en parte se da por la carencia de profesionales como jueces y fiscales afines al tema, que puedan de manera prudente aplicar la correspondiente sanción normativa o dictar el respectivo dictamen fiscal por esta clase de ilícitos.

En Ecuador lo viable es la inclusión de fiscalías especializadas en el tema, y capacitaciones a jueces y fiscales para que tengan mayor conocimiento sobre este tipo de delitos, además para que provean la seguridad jurídica necesaria que todo estado de Derecho necesita de acuerdo a los principios y normas consagradas en la Constitución, la Ley y Tratados Internacionales; podemos tomar como punto de partida y ejemplo el caso de Argentina en la que tienen fiscalías especializadas en delitos informáticos con fiscales de amplia experiencia en la materia, inclusive se puede citar al Dr. Ricardo Sáenz[7], quien es Fiscal General ante la Cámara Nacional de Apelaciones en lo Criminal y Correccional de la Capital Federal, persona de amplia experiencia y renombre en la República de la Argentina.

1.3. Evolución del Delito Informático en Ecuador

> *"El constante progreso tecnológico que experimenta la sociedad, supone una evolución en las formas de delinquir, dando lugar, tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos ilícitos. Esta realidad ha originado los llamados DELITOS INFORMÁTICOS".*[8]

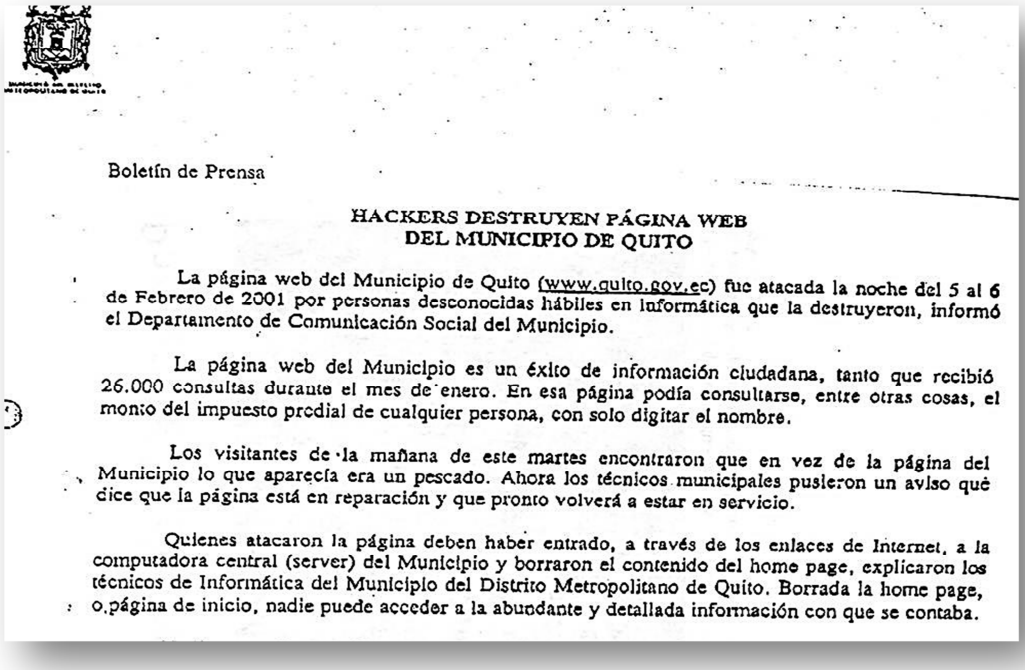
Es así que más allá de los delitos tradicionales se han configurado nuevas formas penales que incluyen dentro de sus elementos principales al Internet como instrumento abstracto, y a la Computadora como instrumento físico.

[7] SÁENZ, Ricardo. "Reforma del Código Penal Argentino"
Internet: http://delitosinformaticos.fiscalias.gob.ar/actualidad/reforma-del-codigo-penal/
Acceso: 17/03/2014
[8] RECOVERY LABS. "Definición de Delito Informático"
Internet: http://delitosinformaticos.info/delitos_informaticos/definicion.html
Acceso: 12/07/2012

Cabe señalar que en el Ecuador se puso en discusión el tema de tipificar y sancionar los delitos informáticos, estas penas que se impondrían las discutieron en el proyecto para la creación de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, proyecto que en principio tuvo ciertas falencias por el desconocimiento de la materia por parte de los legisladores, ya que era una fenómeno criminal que se iniciaba en el país y de la cual se habían reportado pocos casos.

Como antecedente los primeros tipos penales informáticos que se incluyeron en la legislación ecuatoriana fueron en el 2002, en la promulgación de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos[9], artículos que posteriormente fueron incluidos en la reforma del Código Penal ecuatoriano del año 2003. El motivo especial que influyó a que se concluyera con el proyecto de dicha ley, fue uno de los primeros ataques web en el país, que se perpetró en contra de la página del Municipio de Quito en el año 2001, a través de la técnica del hacking conocida como DEFACING[10].

[11]



Boletín de Prensa

HACKERS DESTRUYEN PÁGINA WEB DEL MUNICIPIO DE QUITO

La página web del Municipio de Quito (www.quito.gov.ec) fue atacada la noche del 5 al 6 de Febrero de 2001 por personas desconocidas hábiles en informática que la destruyeron, informó el Departamento de Comunicación Social del Municipio.

La página web del Municipio es un éxito de información ciudadana, tanto que recibió 26.000 consultas durante el mes de enero. En esa página podía consultarse, entre otras cosas, el monto del impuesto predial de cualquier persona, con solo digitar el nombre.

Los visitantes de la mañana de este martes encontraron que en vez de la página del Municipio lo que aparecía era un pescado. Ahora los técnicos municipales pusieron un aviso que dice que la página está en reparación y que pronto volverá a estar en servicio.

Quienes atacaron la página deben haber entrado, a través de los enlaces de Internet, a la computadora central (server) del Municipio y borraron el contenido del home page, explicaron los técnicos de Informática del Municipio del Distrito Metropolitano de Quito. Borrada la home page, o página de inicio, nadie puede acceder a la abundante y detallada información con que se contaba.

[9] REGISTRO OFICIAL. "Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos". Suplemento Oficial N° 557 del 17 de Abril del 2002.

[10] DEFACING: Del español "Desconfigurar", técnica del hacking que consiste en modificar todo o parte del index, es decir la página principal de un sitio web, en dicha modificación o desconfiguración se incluye un logo, mensaje, slogan y contacto del ciberdelincuente que comete el ilícito.

[11] MUNICIPIO DE QUITO. Boletín de Prensa. *"Hackers destruyen página web del Municipio de Quito"*. Fecha: 06-02-2001.

Es necesario recordar que el primer delito informático que se cometió en el Ecuador, fue en el año 1996, en un caso poco conocido que fue denunciado pero que nunca obtuvo sentencia y es sobre el redondeo en las planillas realizadas al antiguo EMETEL[12], de este caso no se sabía a donde se dirigían estas cantidades que muchas veces eran demasiado pequeñas para que cause discusión, pero ya en gran número era una cantidad considerable de dinero, para este tipo de delito informático se utilizó la técnica del hacking llamada Salami o ROUNDING DOWN.[13]

Pagina WEB del Muncipio destruida por 'crackers'

LA INFORMACIÓN que las instituciones tienen en la gran red mundial no están a salvo de atentados. Ni siquiera los programas internos son invulnerables a los ataques de los "cibervándalos".

EL MUNICIPIO de Quito denunció que la página web (www.quito.gov.ec) fue atacada la noche del 5 y 6 del presente mes por personas desconocidas pero hábiles en informática.

Al parecer, ciberpiratas "crackers" (especialistas en romper seguros de la red y destruir toda la información de un programa) lograron ingresar en el sistema y acabar con toda la información allí colocada durante mucho tiempo.

En lugar de la página web aparecía un pez. Inmediatamente, los técnicos iniciaron el arreglo e indicaron que pronto volverá el servicio.

Los técnicos del Municipio explicaron que las personas que atacaron la página lo hicieron a través de los enlaces de internet a la computadora central de la Alcaldía y borraron el contenido.

"Son personas que quieren hacer daño al Municipio. Los hackers, como se conoce a las personas que atacan a las páginas web y que son conocedoras de informática, generalmente, buscan provecho personal o impiden que se difunda la información".

UN CONTENIDO VALIOSO SE HA PERDIDO

● LA PÁGINA web contenía información sobre Quito, sus atractivos turísticos, servicios, incluso, la ciudadanía podía consultar el valor del impuesto predial. Mediante este canal también la ciudadanía puede escribir cartas y enviar invitaciones al alcalde, Paco Moncayo.

En 48 horas funcionará nuevamente la página web y esta vez con más seguridad para evitar este tipo de daños, aseguraron los técnicos.

14

En cuanto a la evolución de los delitos informáticos en el caso ecuatoriano, se encuentran diferentes tipos de delitos realizados a través de plataformas informáticas y medios electrónicos, entre estos se puede citar los siguientes delitos que posteriormente los clasificaré en informáticos y computacionales:

[12] EMETEL: Empresa Ecuatoriana de Telefonía, ente estatal, actualmente disoluta; producto de su disolución nació Andinatel S.A y Pacifictel S.A, empresas de telefonía estatales que actualmente forman CNT (Corporación Nacional de Telecomunicaciones).

[13] ROUNDING DOWN: La técnica del "Salami" es una forma de delito automatizado que consiste en el robo de pequeñas cantidades de activos de un gran número de fuentes, de allí su nombre ya que el método equivale al hecho de tomar rebanadas muy delgadas como un trozo de SALAMI sin reducir significativamente el trozo total, por lo que las víctimas de este tipo de delito no se dan cuenta que están siendo objeto de un robo, o las diferencias que perciben en sus balances (de nóminas, cuentas corrientes, inventarios, etc.) son tan pequeñas que no consideran que vale la pena reclamarlas.
(Fuente: http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf)

[14] DIARIO EL HOY. Archivo Histórico. *"Página web del Municipio de Quito destruida por crackers"*. Fecha: 06-02-2001.

- Banking o Delitos Bancarios en línea.
- Cyber bullying o Acoso escolar electrónico (maltrato psicológico a través de plataformas electrónicas).
- Grooming o Acoso Sexual (a menores por internet).
- Chantaje informático.
- Sabotaje informático (dañar medios informáticos con un fin determinado).
- Ciberterrorismo.
- Narcotráfico (captar mulas a través del internet para lavado de dinero).
- Trata de blancas (engañar mujeres con fines sexuales a través de redes sociales y plataformas virtuales).
- Pornografía intantil (para intercambio de material pornográfico de menores de edad por internet).
- Ciberespionaje o Espionaje informático (filtración y divulgación de información sensible).
- Piratería Informática.
- Usurpación de claves (Keylogging, Phishing a través de spam, scams e ingeniería social).
- Violación de correo electrónico.
- Robo y suplantación de Identidad.
- Falsificación de documentos electrónicos.
- Falsificación de firma digital (certificados electrónicos provenientes de estas).
- Asociación Ilícita (para planeación o simulación de delitos convencionales a través de la red).
- Apropiación indebida (de sistemas informáticos)
- Clonación de tarjetas de crédito
- Delitos tributarios (falsificación electrónica de asientos contables)

CAPITULO II
DELITOS INFORMÁTICOS Y CIBERCRIMINALIDAD

2.1. El Delito Informático

2.1.1. Conceptos de Delito Informático

Aunque no hay una definición específica acerca de "Delito Informático", varios tratadistas y especialistas en el tema han hecho el esfuerzo por dilucidar un concepto claro y conciso respecto a este tipo de ilícitos de la nueva era.

Entre las definiciones más conocidas podemos destacar la del profesor mexicano Julio Telléz Valdés, quien en su obra "Derecho Informático"[15] plasma el concepto de Delito Informático desde dos acepciones, la primera como forma típica entendiendo a *"las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin"*, y la segunda como forma atípica, entendiendo a *"las actitudes ilícitas en las que se tiene a las computadoras como instrumento o fin"*. Así mismo se destaca el concepto de la tratadista Nidia Callegari[16] quien define al Delito Informático como *"aquel que se da con la ayuda de la informática o de técnicas anexas"*, entendiendo como técnicas anexas, a las formas de utilizar las técnicas del hacking para la comisión de ilícitos. Hay que precisar que este concepto no es del todo claro, pues la tratadista sólo toma la informática como medio para la consumación del delito y no como objeto de la infracción.

El Departamento de Investigación de la Universidad de México, señala como delitos informáticos a *"todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio*

[15] TELLÉZ VALDÉS, Julio. Derecho Informático. México D.F, Editorial Mc Graw Hill, 4ª Edición, 2006.
[16] CALLEGARI, Nidia. Citado por: CONDE O'DONNELL, Hugo. "El Delito Informático". Internet: http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf Acceso: 07/06/2013

Informático"[17]. El italiano Carlos Sarzana, define el Delito Informático como *"cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo"*[18].

María de la Luz Lima dice que el delito electrónico en su 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"*.[19] Se puede destacar que dentro de este concepto lo que trata la autora es de hacer una pequeña pero clara diferencia entre lo que es un delito electrónico y un delito informático, confundiendo por la ambigüedad del término al delito informático con el delito computacional, pues brevemente puedo señalar que el delito informático ataca a la información y al dato como bienes jurídicos protegidos, mientras el delito computacional utiliza a la computadora como medio para la comisión del delito, y como objeto de la infracción.

El profesor chileno Renato Jijena Leiva menciona en su obra "Chile, La protección penal a la Intimidad y el Delito Informático" que el delito informático es *"... toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento automatizado de la misma"*.[20]

El experto ecuatoriano en derecho penal informático, Doctor Santiago Acurio del Pino, realiza un aporte importante al mencionar que sin circunscribirse a términos rígidos como delitos informáticos, hace hincapié en el término delincuencia informática para referirse a ellos, indicando que este es *"todo acto o conducta ilícita e*

[17] UNIVERSIDAD NACIONAL DE MÉXICO, Departamento de Investigación. Citado por: VIEGA RODRÍGUEZ, María José. "Un nuevo desafío jurídico: los Delitos Informáticos". Internet: http://mjv.viegasociados.com/wp-content/uploads/2011/05/DelitosInformaticos.pdf Acceso: 05/01/2014

[18] SARZANA, Carlos. Citado por: CONDE O'DONNELL, Hugo. "El Delito Informático". Internet: http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf Acceso: 07/06/2013

[19] DE LA LUZ LIMA, María. Citado por: CONDE O'DONNELL, Hugo. "El Delito Informático". Internet: http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf Acceso: 07/06/2013

[20] LEIVA JIJENA, Renato. *Chile, la protección penal de la intimidad y el delito informático.* Santiago de Chile, Editorial Andrés Bello, 2ª Edición, 1992. Página 225.

ilegal que pueda ser considerada como criminal, dirigida a alterar, socavar, destruir, o manipular cualquier sistema informático o alguna de sus partes componentes, que tenga como finalidad causar una lesión o poner en peligro un bien jurídico cualquiera".[21]

Así mismo el Profesor Santiago Acurio del Pino, destaca que parte importante de la doctrina señala *"que no estamos frente a nuevos delitos, sino más bien ante una nueva forma o formas de llevar a cabo los delitos tradicionales, por lo que no vale individualizarlos de una manera específica, correspondiendo al legislador introducir las modificaciones legales pertinentes a fin de adecuar los tipos penales tradicionales a los nuevos modos de proceder por parte de delincuentes*."[22] De esta manera reduciríamos el excesivo número de tipos penales que existen en la legislación ecuatoriana, adaptando el delito tradicional a las nuevas formas de delinquir por parte de los delincuentes, que en la actualidad hacen uso de la tecnología como su herramienta de trabajo; y lo más importante partiendo del hecho que, más allá de los mecanismos usados para la comisión del delito, está la vulneración del bien jurídico protegido, dando importancia primordial a la información y al dato, mas no exclusividad, pues tenemos otros bienes jurídicos que pueden ser afectados como la seguridad nacional, la intimidad personal, la integridad sexual, el patrimonio, etc.

A esta conclusión, se une el concepto del profesor Enrique Rovira del Canto, quien menciona que el delito informático *"no debe venir referido a la realización de una conducta ilícita a través de elementos o medios informáticos, meramente que éstos sean objeto de tal comportamiento delictivo, sino que debe constituirse en torno a la afectación de la información como bien jurídico protegido, primordial y básico, que no exclusivo. Por tanto, se deberá tener presente si resultan afectados otros bienes jurídicos, normalmente tradicionales"*

De las varias definiciones sobre Delito Informático, se debe tomar una gran e importante diferencia entre los delitos tradicionales por medios informáticos que son los delitos computacionales, y los delitos de la alta tecnología enmarcados como delitos informáticos y encuadrados fuera de lo tradicional.

---

[21] ACURIO DEL PINO, Santiago. *Derecho y Nuevas Tecnologías.* Quito, Corporación de Estudios y Publicaciones, 1ª Edición, 2010. Página 180.
[22] ACURIO DEL PINO, Santiago. *Derecho y Nuevas Tecnologías.* Quito, Corporación de Estudios y Publicaciones, 1ª Edición, 2010. Páginas 177 y 178.

Para concluir, y en razón de lo antes expuesto diré que *"el delito informático es toda actividad delictual en la cual se utilizan sistemas y medios computacionales, telemáticos y electrónicos como medio y fin para el cometimiento de un delito, que principalmente afectan al dato y a la información como bienes jurídicos protegidos. Los delitos informáticos en ciertos casos constituyen nuevos tipos penales que incluyen dentro de sus elementos principales al internet como instrumento abstracto y a la computadora como instrumento físico. El delito informático en sus diferentes tipos y/o facetas, es un delito susceptible de ser sancionado, siempre y cuando la conducta antijurídica se encuentre configurada al tipo y establecida en un cuerpo normativo, llámese Código Penal.*[23]

2.1.2. Delito Informático como MEDIO y FIN

Dentro de los llamados Delitos Informáticos, un tema importarte a resaltar es la manera de cómo son clasificados estos en base a dos criterios: como medio o instrumento, o como fin u objeto.

Citando lo que dice el Profesor Julio Téllez Valdés, como instrumento o MEDIO *"se tienen a las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito"*; mientras que como FIN u objeto *"se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física"*[24].

Si bien el Delito Informático puede ser visto como medio o fin, la importancia que se da a la computadora debe ser vista desde ambos criterios, como medio para consumación del delito, y como fin en relación al objeto material de la infracción, así diríamos que actúa el hardware (instrumento físico), no sin antes necesitar de software (programa, sistema).

[23] El Autor
[24] TÉLLEZ VALDÉS, Julio. Citado por: LEVENE, Ricardo y CHIARAVALLORTI, Alicia. "Introducción a los Delitos Informáticos, tipos y legislación"
Internet: http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml
Acceso: 01/12/2013

2.1.3. Diferencia entre Delito Informático y Delito Computacional

Si partimos del hecho según lo expuesto por el profesor Romero Casabona de que el computador y sus aplicaciones constituyen el objeto material del delito podríamos estar hablando de Delito Informático, mientras que si se lo considera como un mero instrumento para la comisión de actos que generalmente están tipificados en el Código Penal lo encasillaríamos como Delito Computacional, es así que para dilucidar la diferencia entre el concepto del Delito Informático y el Delito Computacional, basta en centrarnos y ver a la computadora como un medio y como fin para hacer una mera diferencia entre estas dos acepciones.

Se dice que los Delitos Informáticos son actos por los cuales se vulnera la información y el dato como bienes jurídicos protegidos, mediante una conducta revestida de los elementos característicos del tipo penal como son la tipicidad, antijuricidad y culpabilidad contra soportes tangibles e intangibles dentro de un sistema de procesamiento de información, llámese programa, software o dato relevante. En cuanto a los Delitos Computacionales podemos decir que son aquellos cometidos por medio del computador empleando las TIC's (Tecnologías de la Información y Comunicación) como medio delictivo para la comisión de delitos tradicionales ya establecidos en el Código Penal.

Concluyendo lo antes dicho, la diferencia esencial radica en que los delitos computacionales utilizan el ordenador (como fin) para cometer delitos ya tipificados en el código penal, es decir delitos tradicionales, y los delitos informáticos se refiere a la comisión de delitos atentando a la información contenida en medios magnéticos y digitales que son realizados a través de la computadora (como medio).

2.2. Naturaleza Jurídica del Delito Informático

Para determinar la naturaleza jurídica del delito informático, debemos partir que es un hecho jurídico, en el cual los múltiples comportamientos irregulares que se dan con el avance de la tecnología, determinan diferentes conductas que permiten la comisión del delito, es por eso que se vuelve necesario buscar la forma o método para hacer de estas conductas un hecho punible.

Los Delitos Informáticos en su mayoría son delitos tradicionales que con la ayuda de la TIC's suponen nuevas formas de delinquir, que conllevan y en ciertos casos a la creación de nuevos tipos penales, y de una nueva conceptualización sobre la tendencia criminal, a su vez deriva en una nueva aplicación del principio de territorialidad por el cometimiento de estos en el medio digital.

2.2.1. Sujetos del Delito Informático

2.2.1.1. Sujeto Activo

En materia penal se dice que el sujeto activo es "*aquella persona que realiza la acción penal prohibitiva u omite la acción penal esperada, que en ciertas circunstancias la ley exige una calidad o condición especial"*.[25]

En delitos informáticos si hablásemos de sujeto activo, es el conocido de forma general por la sociedad como "hacker", quien es la persona con ciertas habilidades para el manejo de sistemas informáticos, y que generalmente por su situación laboral se encuentra en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informáticos, aun cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.[26]

Si hablásemos de personas que por su cargo, rol o manejo de información cometen este tipo de ilícitos actuando desde adentro de la empresa, negocio u organización se los denomina INSIDERS, y los que teniendo un conocimiento amplio en temas informáticos cometen el acto delictivo siendo agentes externos a la empresa, negocio u organización, se los denomina OUTSIDERS.

El problema que respecta en lo relacionado al sujeto activo como ente principal para la comisión de un delito informático, radica en el hecho que la mayoría de ilícitos son cometidos por los llamados INSIDERS, pues por estos se facilita la comisión

[25] SACOTO DE MERLYN, Pilar. *Apuntes de Introducción al Derecho Penal.* Citado por el Autor.
[26] LEVENE, Ricardo y CHIARAVALLORTI, Alicia. "Introducción a los Delitos Informáticos, tipos y legislación"
Internet: http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml
Acceso: 01/12/2013

del delito y la fuga de información, afectado principalmente al dato como bien jurídico tutelado por el Estado.

2.2.1.2. Sujeto Pasivo

Debemos comenzar diciendo que el sujeto pasivo o víctima es la persona o cosa sobre la cual recae la acción antijurídica cometida por el sujeto activo. En materia penal informática, el sujeto pasivo es la víctima del delito informático, sobre la cual recae la acción dolosa producida por el sujeto activo a través de la computadora u objeto telemático con la ayuda de la tecnologías de la información o TIC's.

Hay que tomar presta atención que en la mayoría de casos, la víctima del delito informático es la persona que tiene conocimientos nulos u escasos en informática, por lo cual, por dicho desconocimiento se vuelve presa fácil o vulnerable de los llamados ciberdelincuentes que en la actualidad tienden a atacar a su objetivo después de analizar sus debilidades.

2.3. El Delincuente Informático

2.3.1. Perfil del Delincuente Informático o Ciberdelincuente

Como ya antes he mencionado, el perfil de delincuente informático está revestido de ciertas características que le permiten conducir o perpetrar el delito, características ampliamente técnicas, que ha conciencia y voluntad buscan hacer un daño sobre un bien o una persona en específico para obtener, destruir, alterar o divulgar la información deseada.

Debemos partir del hecho que la palabra hacker es un término ampliamente generalizado, en el cual el común de la sociedad lo hace referencia o comparación a un pirata informático o delincuente, de allí el vocablo ciberdelincuente. Hay que considerar que dentro del Hacking hay una categorización de los sujetos que pertenecen a este fenómeno del Cibercrimen, así tenemos a los hackers, crackers, phreakers, viruckers, piratas informáticos, script kiddie, noob, newbie, lammer, dropper, carder, phisher, cyberstalker y otros; así mismo una clasificación de los llamados hacker principalmente en: hacker negro (blackhat), hacker gris (greyhat), y hacker blanco (whitehat).

2.3.1.1. Categorización de Sujetos en el Hacking

- *Hacker:* Es aquella persona que hace del hacking un arte, descubriendo y creando soluciones tecnológicas que puedan ayudar o beneficiar a un sector estratégico de la sociedad.
  Entre los más conocidos están Bill Gates (CEO de Microsoft), Mark Zuckerberg (Creador de Facebook), Jay Freeman alias Saurik (Creador de Cydia para dispositivos Apple).

- *Cracker:* Se dice de aquella persona dedicada a modificar, alterar o suprimir características esenciales de un programa o software con un fin malicioso o pecuniario.
  Los casos más comunes se dan en programas de paga, en los cuales el Cracker modifica el código del programa de paga para acceder a los beneficios totales del programa sin tener que pagar por la licencia de este. Entre los programas comúnmente crackeados están los antivirus y las versiones del sistema operativo Windows.

- *Phreaker:* Es la persona dedicada al hackeo de redes fijas y móviles.
  El pionero y más conocido Phreaker es John Draper alias Capitán Crunch[27], quien fue el primer hombre es hackear AT&T mediante un silbato.

- *Virucker:* Se dice que es la persona que se encarga del diseño, ensamblaje y creación a través de código malicioso de programas para transmitir o portar virus que infectan a los sistemas informáticos con el propósito de sustraer información o dañar sistemas.
  El más conocido es Robert Tappan Morris por crear el Gusano Morris en 1988, considerado como el primer gusano de ordenador de la era de Internet.[28]

[27] Léase más en: http://www.webcrunchers.com/who-is-john-draper-aka-captain-crunch/
[28] Léase más en: http://es.wikipedia.org/wiki/Robert_Tappan_Morris

- *Pirata Informático:* Es aquella persona que teniendo un conocimiento medio o avanzado de hacking, hace de esta una herramienta de trabajo para el cometimiento de actividades ilegales de tipo económico o financiero.

  En la actualidad hay cientos de piratas informáticos en todo el mundo, en la últimas dos décadas el más renombrado fue Vladimir Levin, quien fue acusado y preso por la Interpol después de meses de investigación por ser la mente maestra de una serie de fraudes tecnológicos que le permitieron a él y la banda que conformaba, substraer más de 10 millones de dólares, de cuentas corporativas del Citibank.

- *Script Kiddie:* Dícese de la persona que plagia y utiliza el código o script perteneciente a otra persona conocedora del hacking, con el fin de utilizar este código alardeando como si fuese de su autoría.

- *Noob o Newbie:* Dícese de la persona novata o principiante en el mundo de hacking, la cual busca adentrarse en este temática con el fin de adquirir nuevos conocimientos en temas relacionados a la seguridad e inseguridad informática.

- *Lammer:* Dícese de la persona que se atribuye ser hacker sin poseer conocimientos de hacking.

- *Dropper:* Es la persona que se dedica a proveer y vender información concerniente a pines de seguridad y códigos CVV de tarjetas de crédito en todo el mundo.

  Normalmente en el mercado negro conocido también como Deep Web se encuentran proveedores o comerciantes que venden estos códigos de tarjetas de crédito. El precio entre comprar un código y pin para clonación de crédito oscila entre los 200 a 300 dólares americanos.

- *Carder:* Se dice que es la persona encargada de clonar tarjetas de crédito, en especial sus bandas magnéticas con un aparato electrónico llamado skimmer.

- *Phisher:* Es la persona que se dedica a clonar sitios web de diferente índole, con el fin de engañar al usuario final para la obtención de información de carácter sensible.

  Normalmente los llamados Phisher se dedican a la clonación de sitios web relacionados a la banca on-line para obtener datos que les permitan acceder a la cuenta del usuario para realizar transferencias bancarias.

- *Cyberstalker:* Dícese de la persona que hace uso del internet para acechar a su víctima sin ser detectado, abusando de la anonimidad que existente en el internet para cumplir con su fin.

  Vulgarmente se dice que el Cyberstalker es la persona que espía a otra a través del internet como en redes sociales con el fin de saber u obtener más información de esta sin que lo sospeche.

2.3.1.2. Clasificación de Hackers

- *Black Hat:* Los llamados Black Hat o hackers de sombrero negro, son aquellos que se encargan de violar la seguridad de sitios web, aplicaciones, base de datos y sistemas automatizados de información con propósito malicioso, a su vez buscan del hacking un pecunio como forma de ganarse la vida.

- *White Hat:* Conocidos como hackers de sombrero blanco o Ethical hackers, se encargan de crear sistemas informáticos y programas con el propósito de beneficiar a un sector en específico de la colectividad, a su vez se encargan de explotar fallas y vulnerabilidades de sistemas informáticos con el fin de recomendar un lineamiento de protección en temas de seguridad de la información.

- *Gray Hat:* Un hacker de sombro gris, es aquel que se perfila entre un hacker negro y un hacker blanco, que ciertas veces actúa en el hacking de forma

ética informando sobre vulnerabilidades y fallas en los sistemas, y otras veces explota estas de forma anti ética para beneficio propio.

2.4. Tipología de Delitos Informáticos

2.4.1. Delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos

2.4.1.1. Acceso ilícito

El delito de acceso ilícito a sistemas informáticos es uno de los delitos informáticos más antiguos. Con el avance y mejora de la tecnología y redes informáticas, especialmente el Internet, este delito ha ido adquiriendo popularidad en el mundo del hacking o underground. Dentro de la historia de los ataques informáticos, en su mayoría han sido a páginas gubernamentales con el propósito de revelar información, o de saber la secreta. De los accesos ilícitos más destacados tenemos a la NASA, Fuerzas Aéreas de Estados Unidos, el Pentágono, Yahoo, Google, Ebay y la Casa Blanca.

El fin de los delincuentes informáticos son diversos, desde burlar las seguridades de un sitio o aplicación web por satisfacción personal hasta extraer y vender datos de estos en el mercado negro. En el caso ecuatoriano, estos delitos se producen en su mayoría a páginas web gubernamentales con el propósito de realizar una protesta virtual conocida también como hacktivismo.

[29]

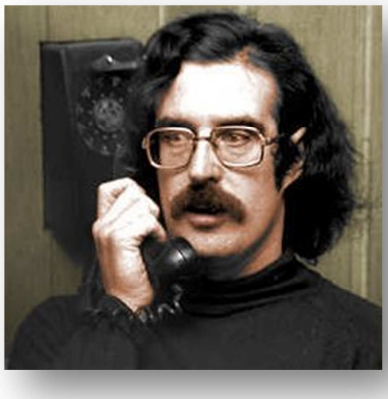
[29] Página web del Departamento de Agricultura de Estados Unidos, atacada por hackers.

2.4.1.2. Intervención ilícita

Con el paso del tiempo los ciberdelincuentes han buscado la forma de intervenir e interceptar datos, además de realizar múltiples delitos con ayuda de dispositivos externos. De los casos frecuentes suscitados años atrás, vemos el de los Phreakers, que eran personas capaces de realizar llamadas con un dispositivo llamado "bluebox", el cual permitía realizar llamadas a destinos internacionales de forma gratuita.

La mayoría de procesos de transmisión de datos e información están resguardados por los proveedores de infraestructura de internet, los mismos que están debidamente protegidos en contra de ataques informáticos por lo que es un tanto difícil intervenirlos.[30] Sin embargo, los ciberdelincuentes buscan las formas y puntos vulnerables para poder inmiscuirse hasta obtener la información deseada en el momento deseado.

Hoy en día la mayoría de lugares tiene conexión a internet, en su mayoría con señal de wifi abierta es decir sin clave, por donde el tráfico de datos de router a dispositivo aunque cifrado no es nada seguro, por lo que, los ciberdelincuentes a través de programas como Wireshark logran medir el tráfico de datos que pasa por la red de la víctima, de forma que es accesible saber qué información está pasando desde y al ordenador de su objetivo.



[31]

[30] INTERNATIONAL TELECOMUNICATION UNION. *Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report.* Ginebra, UN ITU, 1ª Edición, 2008. Página 30. Internet: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html. Acceso: 20-01-2011

[31] John Draper alias Capitán Crunch, primer hacker Phreaker en la historia de Hacking. Pionero en la intervención ilícita de llamadas telefónicas con dispositivos Motorola en Estados Unidos.

2.4.1.3. Manipulación de datos

Los datos informáticos son esenciales para los usuarios privados, las empresas y las administraciones, lo que depende de la integridad y disponibilidad de los datos. La carencia de acceso a los datos puede causar daños (económicos) considerables. Los infractores pueden atentar contra la integridad de los datos de las siguientes formas[32]:

• Borrándolos
• Suprimiéndolos
• Alterándolos
• Restringiendo el acceso a los mismos.

2.4.1.4. Ataques contra la integridad del sistema

Los ataques que se suscitan a sistemas informáticos acarrean las mismas preocupaciones que los ataques a datos informáticos pues, cada uno tiene de por si información delicada y valiosa para la empresa u organización.

La seguridad a la integridad del sistema no solo puede ser a distancia, también se pueden realizar ataques físicos, estos pueden ser realizados por los administradores del sistema quienes tienen acceso al hardware, es decir a los servidores, equipos y demás. Si bien el daño físico se produce, el daño que más afecta es el virtual pues toda la información se logra almacenar en la memoria volátil.

2.4.1.5. Espionaje de datos

Los sistemas informáticos en su mayoría contienen información confidencial por lo tanto delicada que si es substraída para fines delictivos pueden acarrear grandes consecuencias. En cuanto a los sistemas informáticos basta con el mero hecho de tener una computadora y estar conectado al internet para que el ciberdelincuente intente obtener acceso a la información y lo que hay dentro de ella, esto lo puede hacer desde cualquier lugar del planeta de forma remota.

La información protegida y delicada dentro de la web tiende a ser interesante para los ciberdelincuentes, he ahí un primer motivo “la curiosidad”.

[32] INTERNATIONAL TELECOMUNICATION UNION. *El ciberdelito: Guía para los países en desarrollo.* Ginebra, UN ITU, 1ª Edición, 2008. Página 28.
Internet: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf
Acceso: 05-04-2011

En los años ochenta, varios piratas informáticos lograron evadir las seguridades y entraron a los sistemas informáticos militares y de Gobierno de Estados Unidos, muchos de ellos vendieron esta información a agentes de la Ex Unión Soviética.

En la actualidad en los Estados Unidos, se suscitó un caso muy interesante y controversial en donde un agente de inteligencia de Estados Unidos llamado Bradley Manning entregó información secreta de EE-UU a Wikileaks.

Imagen: Diario El Universo, “Bradley Manning, condenado a 35 años de prisión”

2.4.2. Delitos informáticos propios

2.4.2.1. Falsificación informática

Se considera como falsificación informática al hecho de alterar, manipular, eliminar, destruir, modificar un medio digital que puede ser un documento electrónico, imágenes, aplicaciones, etc. Todo este tipo de materiales digitales al querer ser utilizados

como medio probatorio en un juicio y al ser modificados, alterados o destruidos pierden su esencia, pues la manipulación no da credibilidad a estos.

En la legislación ecuatoriana en el Código Penal del 2003, existía un tipo penal en el que señalaba que se impone una pena a quien dañe, suprima o modifique un documento electrónico, sirva este o no como prueba en litis; cabe la duda si en el Ecuador hay el personal adecuado entiéndase Jueces y Fiscales, capaces de conocer que es la prueba digital. Hago este comentario con motivo que dentro de la cadena de custodia que se debe llevar para cubrir la escena de crimen, muchos de los Fiscales que llegan al lugar, no tienen conocimiento suficiente en materia penal informática, por lo que se les dificulta precisar los objetos materia del delito y como se relacionan entre estos para la culminación de la infracción.

2.4.2.2. Fraude informático

Entre los delitos informáticos cometidos en el internet, el fraude informático es uno de los más populares puesto que con la automatización y herramientas informáticas de fácil acceso se pueden encubrir identidades delictivas.[33]

Gracias a la mejora de la tecnología los delincuentes obtienen importante beneficios en el mundo del Cibercrimen, siendo la pérdida para los consumidores alta. En el Cibercrimen los delincuentes informáticos no ven edad, sexo o condición social, lo único que buscan es satisfacer su pretensiones acumulando información de propiedad de otros.

Entre los fraudes de mayor circulación en internet tenemos a las cartas nigerianas que no son más que hoax que pretenden timar a la víctima haciéndole creer cosas falsas que parecen fidedignas, para esto utilizan ingeniería social también conocida como el arte del engaño.

2.4.2.3. Robo y suplantación de identidad

La expresión "robo de identidad", que no se ha definido ni utilizado coherentemente, alude al acto delictivo de obtener y adoptar de forma fraudulenta la

[33] INTERNATIONAL TELECOMUNICATION UNION. *El ciberdelito: Guía para los países en desarrollo.* Ginebra, UN ITU, 1ª Edición, 2008.
Internet: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf

identidad de otra persona. Estos actos pueden cometerse inclusive sin recurrir a medios técnicos o también en línea utilizando la tecnología del Internet.[34]

Por lo general, este delito consta de tres etapas diferentes:

I. En la primera etapa, el delincuente obtiene información relativa a la identidad mediante, por ejemplo, programas informáticos dañinos o ataques destinados como los phishing.
II. La segunda etapa se caracteriza por la interacción con la información obtenida antes de utilizarla en el marco de una actividad delictiva, como ocurre con la venta de ese tipo de información. Se venden, por ejemplo, listas de tarjetas de crédito a un precio alto.
III. La tercera etapa consiste en la utilización de la información relativa a la identidad en relación con una actividad delictiva. En la mayoría de los casos, con el acceso a esos datos los delincuentes pueden perpetrar nuevos delitos y, por ese motivo, dan menos prioridad al conjunto de datos propiamente dicho que a la capacidad para utilizarlos en actividades delictivas. Pueden citarse como ejemplo la falsificación de documentos de identidad o el fraude de las tarjetas de crédito[35].

Según Dmitry Bestuzhev de Kaspersky Lab, de sus charlas dadas en territorio ecuatoriano, nos comenta que sólo en el Ecuador, en cuanto a este tipo de delitos ha ido en aumento, es así que obtener un pasaporte ecuatoriano en el mercado negro oscila entre 400 a 600 USD.

2.4.2.4. Utilización indebida de dispositivos

Cometer un delito informático no es del todo difícil, pues no se requiere una computadora con requisitos específicos para cometerlo. Únicamente se necesita la mera conexión a internet y un ordenador sumamente básico para que el delincuente actué con

[34] INTERNATIONAL TELECOMUNICATION UNION. *El ciberdelito: Guía para los países en desarrollo.* Ginebra, UN ITU, 1ª Edición, 2008. Página 52.
Internet: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf
[35] Ídem

ingenio y obtenga lo deseado. Entre los delitos más fáciles de cometer están el acoso, fraude y difamación informática que se lo puede hacer simplemente desde un cibercafé.

Para el cometimiento de Delitos específicos de mayor magnitud, en cambio se necesitan programas o software con licencia tipo shareware, encontrados fácilmente en la red, otros pueden ser crackeados como es el caso de Havij en su versión 1.3 o 1.5, que sirve al ciberdelincuente para encontrar la base de datos de un sitio web y explotar su vulnerabilidad, otro tipo de delitos requieren técnicas más complejas, citando por ejemplo la INYECCIÓN SQL.[36]

2.5. Tipología de Delitos Computacionales

2.5.1. Delitos relacionados con el contenido

2.5.1.1. Material erótico o pornográfico

Del material comercializado por internet, la pornografía fue una de los primeros, para lo cual a posteriori dio como resultado el intercambio, venta y distribución en la red. Según estadísticas el número de sitios concernientes a contenido sexual explícito asciende a los 4,2 millones.

En Ecuador en relación a este delito, hasta el año 2014 no se encontraba del todo tipificado, pues lo que se penaba era la distribución, venta y grabación de este tipo material, de manera que se incurría en piratería pornográfica.

Para los países que penalizan la interacción con material pornográfico resulta difícil impedir el acceso al mismo. Fuera de Internet las autoridades pueden detectar y enjuiciar las infracciones a la prohibición de material pornográfico. En cambio en Internet el material pornográfico suele figurar en servidores situados fuera del país, por lo que la aplicación de la ley resulta difícil. Aun cuando las autoridades lleguen a identificar los sitios web que contienen el material pornográfico, no tienen la facultad de obligar a los

[36] WIKIPEDIA. "Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabilidad informática presente en una aplicación en el nivel de validación de las entradas para realizar consultas a una base de datos"
Internet: http://es.wikipedia.org/wiki/Inyecci%C3%B3n_SQL
Acceso: 01/12/2013

proveedores a retirar el contenido ofensivo. Por lo general, el principio de territorialidad no permite a un país realizar investigaciones dentro del territorio de otro país sin el permiso de las autoridades locales. Incluso si las autoridades tratan de obtener la ayuda de los países en los que se encuentran ubicados los sitios web ofensivos, el principio de "doble incriminación" puede dificultar el éxito de la investigación y la interposición de sanciones penales. Para impedir el acceso a contenido pornográfico, los países con legislación extremadamente estricta se suelen limitar al bloqueo del acceso a determinados sitios web.[37]

2.5.1.2. Pornografía infantil

Al contrario que en el caso de la pornografía de adultos, donde existe divergencia de opiniones, cuando se trata de pornografía infantil hay unanimidad en su condena y los delitos relacionados con la pornografía infantil se consideran generalmente actos criminales.[38] Diversas organizaciones internacionales se dedican a luchar contra la pornografía infantil en Internet en el marco de varias iniciativas jurídicas internacionales, entre las que cabe citar: la Convención de las Naciones Unidas sobre los Derechos del Niño de 1989[39]; la Decisión Marco del Consejo de la Unión Europea relativa a la lucha contra la explotación sexual de los niños y la pornografía infantil de 2003[40]; y el Convenio del Consejo de Europa, de 2007, sobre la protección de los niños contra la explotación sexual y el abuso sexual.[41]

---

[37] INTERNATIONAL TELECOMUNICATION UNION. *El ciberdelito: Guía para los países en desarrollo.* Ginebra, UN ITU, 1ª Edición, 2008. Página 34.
Internet: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf
Acceso: 05-04-2011

[38] INTERNATIONAL TELECOMUNICATION UNION. "Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report"
Internet: http://www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html.
Acceso: 20-01-2011

[39] UNITED NATIONS. "United Nations Convention of Right of the child.
Internet: http://www.hrweb.org/legal/child.html.
Acceso: 19-03-12

[40] EUROLEX. "Council Framework Decision on combating the sexual exploitation of children and child pornography".
Internet: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_013/l_01320040120en00440048.pdf
Acceso: 20-03-12

[41] COUNCIL OF EUROPE. "Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse".
Internet: http://conventions.coe.int
Acceso: 20-03-12

Lamentablemente, estas iniciativas destinadas a controlar la distribución de pornografía por la red han resultado poco disuasorias para los autores de dicha distribución, que utilizan Internet para comunicarse e intercambiar material de pornografía infantil. El aumento de la anchura de banda ha contribuido al intercambio de archivos de vídeo e imágenes.

Imagen: Caricatura que refleja la perseversión del atacante para atrapar a su víctima.

Según investigaciones sobre el comportamiento de los infractores de pornografía infantil, el 15% de los detenidos por delitos de pornografía infantil por Internet guardaban en su computador más de 1000 imágenes, el 60% de los cuales los niños comprendían edades entre 6 y 12 años, el 19% tenían imágenes de niños menores de 3 años, y el 21% era imágenes de niños con escenas violentas.[42]

2.5.1.3. Incitación al Odio y la Violencia

Muchas personas o grupos radicales usan los medios de comunicación como redes sociales para difundir mensajes de protesta, pero otros sobrepasan estos límites difundiendo mensajes raciales o xenófobos en menosprecio de un grupo en específico de personas, un ejemplo de estos grupos son los llamados “skinheads” o cabezas rapadas,

[42] WOLAK FINKELHOR, Mitchell. "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study"
Internet: http://www.missingkids.com/en_US/publications/NC144.pdf
Acceso: 20-02-2013

quienes incitan al odio en contra de personas a las se les considera diferente por el simple hecho de no pertenecer a su etnia, origen o condición social.

2.5.1.4. Juegos ilegales y juegos en línea

El crecimiento de los juegos en línea en los últimos años se ha incrementado en un 400%, incrementando del mismo modo la posibilidad de delinquir cibernéticamente, un ejemplo claro de esto es el juego on-line llamado Second Life, en el mismo y que según investigaciones, se realizaban algunos delitos entre los cuales estaban e intercambio de material pornográfico infantil, fraude, casinos en línea, entre otros.

En relación juegos on-line ilegales podemos destacar al de los casinos pues, estos además de manejar millones de dólares al año, además burlan las prohibiciones del juego. La proliferación de los casinos va en aumento siendo que la mayoría de estos se encuentran en países con legislación liberal o sin normativa sobre el juego de azar por internet, es así que los usuarios pueden abrir cuentas en línea, transferir dinero y participar en juegos de azar a cualquier hora y día del año.

Según la UIT los casinos en línea también se han utilizado para lavar dinero y financiar el terrorismo, algo que aunque difícil de creer es cierto. Los modus operandi hoy en día en cuanto a estos delitos buscan nuevos blancos y formas de delinquir de manera progresiva, evitando incluso que la misma policía en todo el mundo los pueda perseguir.

2.5.1.5. Difamación e información falsa

De la misma manera que se divulga información fidedigna por internet, así mismo se puede divulgar información falsa, si bien puede ser de las dos formas aquí lo que se busca es una finalidad hacia el target o blanco para beneficiarse sobre algo.

En el caso de la divulgación o difamación de información falsa, ésta en un 90% tiene como objetivo llamar la atención del cibernauta para lograr la veracidad en contra de algo o alguien, normalmente esto se lo suele ver en salas de chat o foros, donde personas anónimas difaman a alguien o simplemente divulgan información falsa en desprestigio de una persona, empresa, producto, marca, etc.

2.5.1.6 Correo basura (spamming) y amenazas conexas

El spam o correo basura se entiende como el envío de mensajes no solicitados, estos normalmente traen información errónea como mensajes de lotería, cadenas sobre personas enfermas o simplemente mensajes sobre víctimas de personas en África, a estas últimas se les conoce normalmente como cartas nigerianas. El correo basura en la actualidad ocupa un enorme tráfico en la red, pues a diario muchos e-mail son perfectos blancos para recibir este tipo de correos.

En el Ecuador el spam ha sido utilizado por empresas de e-marketing para divulgar material publicitario, y por ciberdelincuentes para enviar información fraudulenta sobre avisos bancarios a los clientes de diferentes bancos, con el fin que estos caigan en su trampa y para tener acceso a su información. De los más conocidos, está el spam que llega a diario sobre “avisos importantes” que envía supuestamente Banco del Pichincha, pero que en su realidad son enviados por ciberdelincuentes para obtener la información bancaria de la víctima, para acceder a su cuenta y realizar desvíos bancarios.

Cabe destacar que según investigaciones, algunas empresas ecuatorianas dedicadas al e-marketing, venden su bases de datos de clientes entre 70 a 90 USD a redes de ciberdelincuentes, esto para que se materialice a posteriori el fin delictivo.

2.5.1.7. Otras formas de contenido ilícito

Entre otras formas de contenido ilícito que pueden ser susceptibles de darse por internet, tienen que ver las relacionadas a los delitos contra la vida, en el caso concreto el sicariato. En la red con tan solo escribir la palabra “sicario” más la “ciudad” en el buscador Google, aparecen una serie de anuncios sobre personas que ofrecen su servicio de sicarios a cambio de una suma de dinero, que no siempre es alta.

En el internet entre otros delitos, vemos los relacionados hacia la compra-venta, así mismo encontramos que se ofrece la compra o venta de forma clandestina de órganos del cuerpo humano, los cuáles dependiendo el órgano, llegan a tener un precio de hasta 150.000 USD.

2.5.2. Delitos en materia de derechos de autor y de marcas

2.5.2.1. Delitos en Derechos de Autor

Con el paso del tiempo los sistemas analógicos han cambiado a los digitales permitiendo a la industria del ocio incorporar en materiales DVD, Blue Ray nuevos servicios y prestaciones como subtítulos, idiomas, escenas adicionales y más.

La digitalización ha dado paso a nuevas violaciones de los derechos de autor fundadas en la reproducción rápida y exacta. Entre las violaciones de los derechos de autor más comunes pueden mencionarse las siguientes:

- Intercambio, en sistemas de intercambio de archivos, de programas informáticos, archivos y temas musicales protegidos con derechos de autor
- Elusión de los sistemas de gestión de derechos en el ámbito digital.

El tráfico entre tecnologías y su reproducción en la red representa un papel protagónico puedes en la actualidad es tan fácil acceder y encontrar música o películas en la red gratuitamente descargables.

2.5.2.2. Delitos en derechos de marcas

Los derecho de autor y los derecho de marcar guardan una íntima relación en el sentido en que a los dos se les plagia el contenido ya se descargándolo gratuitamente del internet u obteniendo un copia exacta del mismo.

Las violaciones en materia de marcas se han incorporado al ciberespacio y, en el marco de diferentes Códigos Penales, su tipificación como delito presenta diversos grados. Los delitos más graves son, entre otros[43]:

• La utilización de marcas en actividades delictivas con el propósito de engañar a las víctimas; y

• Los delitos en materia de dominios y nombres.

[43] INTERNATIONAL TELECOMUNICATION UNION. *El ciberdelito: Guía para los países en desarrollo.* Ginebra, UN ITU, 1ª Edición, 2008. Página 48.
Internet: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf
Acceso: 05-04-2011

La buena reputación de una empresa está relacionada por lo general a su marca. Los delincuentes utilizan nombres genéricos y marcas de forma fraudulenta en numerosas actividades, por ejemplo la peska[44], en las que se envían a los usuarios de Internet millones de correos electrónicos similares a los de empresas legítimas, por ejemplo consignando su marca. Otro aspecto de las violaciones de marcas son los delitos en materia de dominios, por ejemplo la ciberocupación ilegal, que describe el procedimiento ilegal de registrar un nombre de dominio idéntico o similar al de la marca de un producto o de una empresa.[45]

2.5.3. Combinación de delitos informáticos

2.5.3.1. Ciberguerra

La ciberguerra o guerra informática se entiende a la utilización de las tecnologías de la información con el propósito de atacar o declarar una guerra en el ciberespacio, estas guerras informáticas por lo general son cometidas por Estados o por grupos de hacking rivales que pelean por territorio en la red.

Teniendo en cuenta tanto las comunicaciones civiles como militares, la infraestructura de la información constituye un objetivo fundamental en los conflictos armados. Sin embargo, no es seguro que esos ataques se cometan por Internet. Los ataques perpetrados a sistemas informáticos en Estonia y los Estados Unidos han sido asociados a la guerra informática. Dada la imposibilidad de determinar a ciencia cierta si un ataque procede de un organismo público oficial, resulta difícil catalogarlo de guerra informática. Ocurre lo mismo con respecto a los ataques físicos -por ejemplo, mediante armas y explosivos - contra infraestructuras.[46]

2.5.3.2. Ciberterrorismo

Desde 2001 el ciber terrorismo también conocido como terrorismo virtual se ha convertido en uno de los novedosos delitos de los criminales informáticos los cuales

[44] PESKA: La peska o phishing, describe una serie de actos llevados a cabo para que las víctimas revelen información personal a través de técnicas usadas con ingeniería social.
[45] INTERNATIONAL TELECOMUNICATION UNION. *El ciberdelito: Guía para los países en desarrollo.* Ginebra, UN ITU, 1ª Edición, 2008. Página 48.
Internet: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf
Acceso: 05-04-2011
[46] Ídem

deciden atacar masivamente el sistema de ordenadores de una empresa, compañía, centro de estudios, oficinas oficiales, etc. Un ejemplo de ello lo ofrece un hacker de Nueva Zelandia, Owen Thor Walker alias AKILL, quien en compañía de otros hackers, dirigió un ataque en contra del sistema de ordenadores de la Universidad de Pennsylvania en 2008.[47]

La difusión de noticias falsas en Internet (por ejemplo decir que va a explotar una bomba en el Metro), es considerado terrorismo informático y es procesable por alterar el orden público.

2.5.3.3 Lavado de dinero

El lavado de dinero a través de internet, es uno de los delitos computacionales que está en auge, pues a diario los ciberdelincuentes no solo buscan mulas para el lavado de dinero, sino también socios de negocios ilícitos a quienes puedan hacer transferencias altas de dinero a cambio de una promesa o dádiva.

La automatización de proceso en los servicios financieros y su rapidez en cuanto a transacciones electrónicas han incentivado para que los ciberdelincuentes se confíen de estos y los utilicen a diario para sus ilícitos.

[47] INFORMÁTICA FORENSE COLOMBIA. “Terrorismo virtual” Internet:www.informaticaforense.com.co/index.php?option=com_content&view=article&id=88&Itemid=90
Acceso: 15-04-2012

CAPITULO III
DELITOS INFORMÁTICOS EN LA LEGISLACIÓN ECUATORIANA

3.1. Tipos penales relacionados a los delitos informáticos y computacionales en el Código Orgánico Integral Penal

En el Registro Oficial N°180 del 10 de Febrero del 2014, se publica el Código Orgánico Integral Penal COIP, en el cual se tipifican nuevas conductas, entre estas las informáticas. En el siguiente capítulo se señalan los tipos penales relacionados a delitos informáticos y computacionales, de los cuales destacan los siguientes:

3.1.1. Tráfico de órganos.-

Artículo 96.- La persona que, fuera de los casos permitidos por la ley, realice actos que tengan por objeto la intermediación onerosa o **negocie por cualquier medio**[48] o traslade órganos, tejidos, fluidos, células, componentes anatómicos o sustancias corporales, será sancionada con pena privativa de libertad de trece a dieciséis años.

3.1.2. Pornografía con utilización de niñas, niños o adolescentes.-

Artículo 103.- La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, **informáticos, electrónicos o de cualquier otro soporte** [49]físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual; será sancionada con pena privativa de libertad de trece a dieciséis años.

Si la víctima, además, sufre algún tipo de discapacidad o enfermedad grave o incurable, se sancionará con pena privativa de libertad de dieciséis a diecinueve años.

Cuando la persona infractora sea el padre, la madre, pariente hasta el cuarto grado de consanguinidad o segundo de afinidad, tutor, representante legal, curador o pertenezca al

[48] En la actualidad se da el tráfico de órganos a través de internet; lo más común es realizado por mafias o bandas dedicadas a esto en el viejo continente especialmente en Holanda, España y Alemania.

[49] Revisar documental "Pederastas en la Red". https://www.youtube.com/watch?v=C69lFrtTbs8

entorno íntimo de la familia; ministro de culto, profesor, maestro, o persona que por su profesión o actividad haya abusado de la víctima, será sancionada con pena privativa de libertad de veintidós a veintiséis años.

3.1.3. Comercialización de pornografía con utilización de niñas, niños o adolescentes.-

Artículo 104.- **La persona que publicite, compre, posea, porte, transmita[50], descargue, almacene, importe, exporte o venda, por cualquier medio**, para uso personal o para intercambio pornografía de niños, niñas y adolescentes, será sancionada con pena privativa de libertad de diez a trece años.

3.1.4. Ataque a persona protegida con fines terroristas.-

Artículo 126.- La persona que, con ocasión y en desarrollo de conflicto armado, **realice cualquier forma de ataque**[51] a persona protegida con el objeto de aterrorizar a la población civil será sancionada con pena privativa de libertad de diez a trece años.

3.1.5. Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.-

Artículo 173.- **La persona que a través de un medio electrónico o telemático** proponga concertar un encuentro con una persona menor de dieciocho años, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento con finalidad sexual o erótica, será sancionada con pena privativa de libertad de uno a tres años.

Cuando el acercamiento se obtenga mediante coacción o intimidación, será sancionada con pena privativa de libertad de tres a cinco años.

La persona que suplantando la identidad de un tercero o mediante el uso de una identidad falsa por medios electrónicos o telemáticos, establezca comunicaciones de contenido sexual o erótico con una persona menor de dieciocho años o con discapacidad, será sancionada con pena privativa de libertad de tres a cinco años.

[50] La transmisión de estos se comente a diario, entre los casos conocidos en Ecuador tenemos a GIGATRIBE, una red de pedófilos que a través de una aplicación en el internet llamada GIGATRIBE, mantenía alojados más de 200GB de pornografía infantil.

[51] Tal es el caso de bombas que se activan a través de pulsaciones electromagnéticas empleando un computador, laptop o celular a distancia.

3.1.6. Violación a la intimidad.-

Artículo 178.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en **soportes informáticos**[52], **comunicaciones privadas o reservadas de otra persona por cualquier medio,** será sancionada con pena privativa de libertad de uno a tres años.

No son aplicables estas normas para la persona que divulgue[53] grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.

3.1.7. Calumnia.-

Artículo 182.- La persona que, por cualquier medio, realice una falsa imputación de un delito en contra de otra, será sancionada con pena privativa de libertad de seis meses a dos años.

No constituyen calumnia los pronunciamientos vertidos ante autoridades, jueces y tribunales, cuando las imputaciones se hubieren hecho en razón de la defensa de la causa.

No será responsable de calumnias quien probare la veracidad de las imputaciones. Sin embargo, en ningún caso se admitirá prueba sobre la imputación de un delito que hubiere sido objeto de una sentencia ratificatoria de la inocencia del procesado, de sobreseimiento o archivo.

No habrá lugar a responsabilidad penal si el autor de calumnias, se retractare voluntariamente antes de proferirse sentencia ejecutoriada, siempre que la publicación de la retractación se haga a costa del responsable, se cumpla en el mismo medio y con las mismas características en que se difundió la imputación.

La retractación no constituye una forma de aceptación de culpabilidad.

3.1.8. Estafa.-

Artículo 186.- La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u

[52] El típico caso es el Keylogger, éste es un programa instalado discretamente en la PC de la víctima que capta todas sus pulsaciones electrónicas como cuentas bancarias, cuentas de e-mail y datos; además que captura cada cierto tiempo tomas de pantalla de lo que se está haciendo.

[53] En la mayoría de casos la información que se entiende que es delicada porque no es de libre circulación en la red, es publicada por ciberdelincuentes que han penetrado sitios web o e-mails a través de una web de publicación de datos llamada PASTEBIN (www.pastebin.com)

ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años.

La pena máxima se aplicará a la persona que:

1. Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo consentimiento de su propietario.

2. Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copias o reproducir información de tarjetas de crédito, débito, pago o similares.

3.1.9. Aprovechamiento ilícito de servicios públicos.-

Artículo 188.- **La persona que ofrezca, preste o comercialice servicios públicos** de luz eléctrica, **telecomunicaciones** o agua potable sin estar legalmente facultada, mediante concesión, autorización, licencia, permiso, convenios, registros o cualquier otra forma de contratación administrativa, será sancionada con pena privativa de libertad de uno a tres años.

3.1.10. Apropiación fraudulenta por medios electrónicos.-

Artículo 190.- **La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno** o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.

3.1.11. Reprogramación o modificación de información de equipos terminales móviles.-

Artículo 191.- La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.

3.1.12. Intercambio, comercialización o compra de información de equipos.-

Artículo 192.- La persona que intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.

3.1.13. Reemplazo de identificación de terminales móviles.-

Artículo 193.- La persona que reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la original, será sancionada con pena privativa de libertad de uno a tres años.

3.1.14. Comercialización ilícita de terminales móviles.-

Artículo 194.- La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.

3.1.15. Infraestructura ilícita.-

Artículo 195.- La persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil, será sancionada con pena privativa de libertad de uno a tres años.

No constituye delito, la apertura de bandas para operación de los equipos terminales móviles.

3.1.16. Supresión, alteración o suposición de la identidad y estado civil.-

Artículo 211.- **La persona que ilegalmente impida, altere, añada o suprima la**

inscripción de los datos de identidad suyos o de otra persona en programas informáticos, partidas, tarjetas índices, cédulas o en cualquier otro documento emitido por la Dirección General de Registro Civil, Identificación y de Cedulación o sus dependencias o, inscriba como propia, en la Dirección

General de Registro Civil, Identificación y de Cedulación a una persona que no es su hijo, será sancionada con pena privativa de libertad de uno a tres años.

3.1.17. Suplantación de identidad.-

Artículo 212.- La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años.

3.1.18. Tráfico ilícito de migrantes.-

Artículo 213.- La persona que, con el fin de obtener directa o indirectamente beneficio económico u otro de orden material por cualquier medio[54], promueva, capte, acoja, facilite, induzca, financie, colabore, participe o ayude a la migración ilícita de personas nacionales o extranjeras, desde el territorio del

Estado ecuatoriano hacia otros países o viceversa o, facilite su permanencia irregular en el país, siempre que ello no constituya infracción más grave, será sancionada con pena privativa de libertad de siete a diez años.

3.1.19. Revelación ilegal de base de datos.-

Artículo 229.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes**, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto**, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que

[54] En redes sociales especialmente Facebook, existen redes organizadas que se dedican a engañar mujeres con el propósito de trata de blancas en diferentes países.

realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

3.1.20. Interceptación ilegal de datos.-

Artículo 230.- Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.

2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.

3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.

4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

3.1.21. Transferencia electrónica de activo patrimonial.-

Artículo 231.- **La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos,** para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un

activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

3.1.22. Ataque a la integridad de sistemas informáticos.-

Artículo 232.- **La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos**, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

3.1.23. Delitos contra la información pública reservada legalmente.-

Artículo 233.- La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.

La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

3.1.24. Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.-

Artículo 234.- **La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones** o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

3.1.25. Defraudación tributaria.-

Artículo 298.- La persona que simule, oculte, omita, falsee o engañe en la determinación de la obligación tributaria, para dejar de pagar en todo o en parte los tributos realmente debidos, en provecho propio o de un tercero, será sancionada cuando:

8. **Altere libros o registros informáticos** de contabilidad, anotaciones, asientos u operaciones relativas a la actividad económica, así como el registro contable de cuentas, nombres, cantidades o datos falsos.
9. **Lleve doble contabilidad con distintos asientos en libros o registros informáticos**, para el mismo negocio o actividad económica.
10. **Destruya total o parcialmente, los libros o registros informáticos** de contabilidad u otros exigidos por las normas tributarias o los documentos que los respalden, para evadir el pago o disminuir el valor de obligaciones tributarias.

3.1.26. Defraudación aduanera.-

Artículo 299.- La persona que perjudique a la administración aduanera en las recaudaciones de tributos, sobre mercancías cuya cuantía sea superior a ciento cincuenta salarios básicos unificados del trabajador en general, será sancionada con pena diez veces el valor de los tributos que se pretendió evadir, si realiza cualesquiera de los siguientes actos:

6. Induzca, por cualquier medio, al error a la administración aduanera en la devolución condicionada de tributos.

3.1.27. Producción, tenencia y tráfico de instrumentos destinados a la falsificación de moneda.-

Artículo 305.- La persona que produzca, conserve, adquiera o comercialice materias primas o instrumentos destinados a la falsificación, fabricación o alteración de moneda nacional o extranjera, cheques, títulos valores, tarjetas de crédito, débito, pago u otros documentos o dispositivos empleados como medio de pago equivalente a la moneda, será sancionada con pena privativa de libertad de tres a cinco años.

3.1.28. Falsificación de moneda y otros documentos.-

Artículo 306.- La persona que falsifique, fabrique o adultere moneda de curso legal nacional o extranjera, ponga en circulación o use fraudulentamente efecto oficial regulado por el Estado, será sancionada con pena privativa de libertad de cinco a siete años.

La persona que cometa falsedad forjando en todo o en parte efectos, cheques, títulos valores, tarjetas de crédito, débito o pago, dispositivos empleados como medio de pago equivalente a la moneda o haciendo verdadera cualquier alteración que varíe su sentido o la información que contienen, será sancionada con pena privativa de libertad de cinco a siete años.

3.1.29. Espionaje.-

Artículo 354.- La o el servidor militar[55], policial o de servicios de inteligencia que en tiempo de paz realice uno de estos actos, será sancionado con pena privativa de libertad de siete a diez años, cuando:

1. Obtenga, difunda, falsee o inutilice información clasificada legalmente y que su uso o empleo por país extranjero atente contra la seguridad y la soberanía del Estado.
2. Intercepte, sustraiga, copie información, archivos, fotografías, filmaciones, grabaciones u otros sobre tropas, equipos, operaciones o misiones de carácter militar o policial.
3. Envíe documentos, informes, gráficos u objetos que pongan en riesgo la seguridad o la soberanía del

Estado, sin estar obligado a hacerlo o al haber sido forzado no informe inmediatamente del hecho a las autoridades competentes.

[55] Revisar caso de espionaje militar del agente de inteligencia “Bradley Manning” quien entregó información confidencial de EE-UU a Wikileaks

3.1.30. Apología.-

Artículo 365.- **La persona que por cualquier medio**[56] haga apología de un delito o de una persona sentenciada por un delito, será sancionado con pena privativa de libertad de quince a treinta días.

3.1.31. Contravenciones de cuarta clase.-

Artículo 396.- Será sancionada con pena privativa de libertad de quince a treinta días:

1. La persona que, por cualquier medio, profiera expresiones en descrédito o deshonra en contra de otra.

Esta contravención no será punible si las expresiones son recíprocas en el mismo acto.

3.2. Cuerpos normativos que amparan al usuario frente a ilícitos informáticos y computacionales

Dentro del marco normativo ecuatoriano, hay ciertas leyes, reglamentos y resoluciones que amparan o ayudan al usuario en defensa de sus derechos, cuando estos han sido vulnerados, entre estos tenemos:

- Constitución de la República de Ecuador
- Código Orgánico Penal Integral
- Código Civil
- Código de Procedimiento Civil
- Ley de Propiedad Intelectual
- Ley de Garantías Jurisdiccionales
- Resolución SBS JB-2011-1923 “Controles en los cajeros automáticos”
- Ley de la protección de datos
- Ley de protección de usuarios del sistema financiero
- Ley de derechos de autor

[56] Dentro del contexto del Odio en la historia se han suscitado casos donde se han hecho manifestaciones raciales y peyorativas en contra de ciertos grupos, en el caso concreto entre los hechos realizados por internet tenemos el de las manifestaciones “neo-nazis” en contra de sus diferentes.

- Ley especial de telecomunicaciones
- Ley Orgánica de Transparencia y Acceso a la Información Pública
- Ley Orgánica de Comunicación

CAPITULO IV
PROCESO PENAL EN EL DELITO INFORMÁTICO

Dentro del proceso penal por delito informático debemos tomar varias consideraciones, entre estas las relacionadas a la jurisdicción y competencia de los hechos suscitados en territorio digital, la acción penal que versa en delitos informáticos y computacionales, la denuncia y la acusación particular, el rol de los sujetos procesales principales y auxiliares, la cadena de custodia, la investigación de la escena del crimen y los elementos de convicción y punibilidad.

4.1. Proceso Penal

4.1.1. Jurisdicción y Competencia en territorio digital

Se dice que la jurisdicción es la potestad pública de juzgar y hacer ejecutar lo juzgado, potestad que nace de la voluntad del pueblo soberado, debemos denotar que en materia penal informática, y al conocer que los delitos del tema tratado son cometidos en ciertos casos a través de redes informáticas se hace un tanto complicado o engorroso conocer la procedencia y exactitud del lugar de su cometimiento. Es así que si recordamos el tan conocido principio de territorialidad, este señala y por conocimiento básico en materia penal, que la jurisdicción y competencia versan sobre el lugar de cometimiento del ilícito, es decir donde se cometió el delito y reposa el bien jurídico afectado, ahora en lo relacionado al delito informático, y como bien lo he señalado antes, no se puede diferenciar con exactitud el lugar exacto donde se cometió, en un primer momento; por lo tanto en jurisdicción y competencia en materia penal informática y al desconocerse el lugar de procedencia del ilícito, debe aplicarse la jurisdicción de lugar de los bienes jurídicos afectados, hasta hallar la procedencia a través de medios e investigaciones informáticas que den con el paradero del ataque in situ.

4.1.2. Acción penal

El Código Orgánico Integral Penal que entrará en vigencia el 10 de Agosto del 2014, toma en consideración la acción penal en dos tipos: acción pública mediante

denuncia y la acción privada mediante querella, dejando a un lado las conocidas acción pública de instancia oficial, acción pública de instancia particular y acción privada.

En cuanto a la acción pública, su titularidad le corresponde a la Fiscalía General del Estado, sin denuncia previa, mientras que la titularidad de la acción privada le corresponde a la víctima mediante querella.

4.1.3. Denuncia y acusación particular

DENUNCIA:

La persona que llegue a conocer del cometimiento de un delito de acción pública, puede presentar la correspondiente denuncia en la Fiscalía, en el Sistema especializado integral de investigación (Dirección de Investigaciones de la FGE), en Medicina Legal o ante el correspondiente órgano en materia de tránsito.

Se debe tomar en cuenta que ciertas personas por atribución de la ley tienen el deber de denunciar, entre están los servidores y funcionarios públicos, los profesionales de salud, y los directores y educadores responsables de instituciones educativas.

ACUSACIÓN PARTICULAR:

Podrá presentar la correspondiente acusación particular, la víctima como persona natural por sí misma o a través de su representante o apoderado, la víctima si fuese persona jurídica a través de su representante legal, y la entidad u organismo perteneciente al sector público a través de su procurador, representante legal, delegados especiales o el Procurador General del Estado.

4.1.4. Sujetos procesales principales y auxiliares

SUJETOS PRINCIPALES:

La Fiscalía:

El Fiscal es la persona quien dirige la investigación pre procesal y procesal del delito e interviene como representante del Estado hasta la finalización del proceso. En la resolución e investigación del delito informático el Fiscal cumple un rol muy importante,

pues a través de este se hacen todas las diligencias investigativas en pro de esclarecer el delito, para algunas previamente se necesita de orden judicial, únicamente no se necesitará de orden judicial para aquellas en las que el Fiscal tenga atribución o potestad directa. En el caso de los delitos informáticos, y para el esclarecimiento del delito, depende mucho de la experiencia del Fiscal, el conocimiento que tenga de la materia penal informática, y de la idea de cómo llevar el proceso para conseguir los elementos que le sean favorables para su dictamen frente al Juez. Debemos denotar que lamentablemente en el Ecuador, existen pocos Fiscales que conocen y pueden manejar casos relacionados a delitos informáticas, ya que por cierto desconocimiento de la materia especialmente, hay esos vacíos de cómo actuar o qué pedir frente a la investigación, por lo que los resultados esperados por la víctima en su mayoría son desfavorables.

La Víctima:

Es la persona perjudicada o el sujeto víctima de la agresión, ya sea ésta cometida en un medio físico o virtual, se dice que la víctima es el sujeto pasivo del delito, y como ya lo mencioné antes a través de esta disertación, es la persona o cosa sobre la cual recae la acción antijurídica cometida por el sujeto activo. En materia penal informática, el sujeto pasivo es la víctima del delito informático, sobre la cual recae la acción dolosa producida por el sujeto activo a través de la computadora u objeto telemático con la ayuda de la tecnologías de la información o TIC's.

La persona procesada:

La persona procesada o sujeto activo es aquella a la que se la imputado un delito por no acatar u obedecer, es decir contradecir las normas del ordenamiento jurídico, violentando, dañando o perjudicando a otra persona, animal, cosa o institución. En materia penal se dice que el sujeto activo es "*aquella persona que realiza la acción penal prohibitiva u omite la acción penal esperada, que en ciertas circunstancias la ley exige una calidad o condición especial"*.[57]

En delitos informáticos si hablásemos de sujeto activo, es el conocido de forma general por la sociedad como "hacker", quien es la persona con ciertas habilidades

[57] SACOTO DE MERLYN, Pilar. *Apuntes de Introducción al Derecho Penal.* Citado por el Autor.

para el manejo de sistemas informáticos, y que generalmente por su situación laboral se encuentra en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informáticos, aun cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos.[58]

La Defensa:

Dentro del delito informático, el rol del abogado ya sea designado por la defensoría pública o contratado de forma privada es sumamente importante, en primer término porque no todos los abogados son conocedores o empíricos en la materia penal informática, y en segundo término porque el abogado a través de escrito puede solicitar todo de lo que se crea asistido con el fin de garantizar los derechos de su cliente, y dar una solución al conflicto. La ventaja que lleva un abogado conocedor o especialista en la materia penal informática, es que este conoce el proceso y el resultado que puede obtener solicitando cosas que normalmente un abogado no lo haría, pues el dominio de las técnicas y soluciones a este tipo de conflicto se encasillan dentro de los delitos de la nueva era, así el abogado no sólo conoce de leyes, sino también lo técnico, estando a la par del avance de la tecnología y de los nuevos modos de operar de los delincuentes.

SUJETOS AUXILIARES

La Policía Judicial:

Se considera Policía Judicial o PJ a la entidad adscrita a la Policia Nacional del Ecuador, encargada de prestar los servicios al poder judicial llámeme Función Judicial y la Fiscalía General del Estado para la investigación de delitos y ejecución de sentencia, para la investigación de delitos que pueden ser de distinta índole tales como narcotráfico, trata de blancas, prostitución, pornografía infantil y todos los que tengan que ver con el crimen organizado, y en la ejecución de sentencia para facilitar la aprehensión de los ciudadanos que teniendo sentencia ejecutoriada hagan caso omiso a la ley, evadiéndola o en estado de fuga.

[58] LEVENE, Ricardo y CHIARAVALLORTI, Alicia. “Introducción a los Delitos Informáticos, tipos y legislación”
Internet: http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml
Acceso: 01/12/2013

La Policía Judicial en el Ecuador, es un ente muy importa, que presta la ayuda necesaria para la investigación de crimen, tanto en la fase pre procesal penal como en las etapas penales.

Los peritos:

Un Perito Judicial Informático es el profesional, que en su carácter de auxiliar de la justicia, tiene la función de asesorar al juez respecto a temas informáticos. La función del perito informático consiste en analizar elementos informáticos, en busca de aquellos datos que puedan constituir una prueba o indicio útil para el litigio jurídico al que ha sido asignado.[59]

El Perito Judicial Informático es el que da la aceptación de la veracidad y contundencia de las pruebas presentadas en un proceso legal, encargado de solucionar aspectos de conocimientos que el juez o los tribunales no están obligados a conocer.

El Perito Judicial Informático, tiene que ser experto y tener conocimientos forenses, de investigación legal y criminalística; siendo de vital importancia que esté familiarizado con las pruebas electrónicas. Actualmente se observa la convergencia de técnicas de análisis, estrategias y procedimientos científicos que se disponen para obtener, revisar, analizar y salvaguardar la exactitud y la confiabilidad de este tipo de evidencia. Se destaca que para que el informe presentado por el Perito Informático surta validez, este tiene que estar registrado como perito en la listas o base de datos de la Función Judicial del Consejo Nacional de la Judicatura.

Los testigos:

El testigo es la persona por la cual se conoce cierta vivencia o experiencia relativa al delito, cuyo testimonio ayuda a corroborar ciertos puntos del delito o ayuda a esclarecer como sucedió éste. Las declaraciones vertidas por los testigos en etapa de prueba, y al ser practicados en audiencia pública, oral o contradictoria constituyen elemento de prueba, en contra o en favor del imputado. Es así que el testimonio es pieza fundamental e importantísima dentro del proceso penal.

[59] UNIVERSIDAD DE SALAMANCA. “Qué es un perito informático?”.
Internet: http://diarium.usal.es/salamandra/informatica/%C2%BFque-es-un-perito-informatico/
Acceso: 05-09-2013

Los investigadores civiles, analistas y agentes de inteligencia

Si bien antes se señaló que la Policía Judicial es un sujeto auxiliar del proceso penal, esta nombra un investigador perteneciente a Criminalística, quien ayuda al Fiscal con las investigaciones de campo con el fin de recolectar toda evidencia para comprobar la existencia del delito, y para esclarecer cómo se dio el delito. En casos de mayor magnitud y donde se comete otro tipo de delito como por ejemplo, el terrorismo cibernético, incursará en la investigación agentes de inteligencia, quienes se encargarán de investigar más a fondo el caso, utilizando otros mecanismos y técnicas para hallar la vinculación del objetivo con otros entes criminales, para así desestabilizar o dar un golpe a la organización criminal cuando esta no se lo espera. Cuando el agente de campo haga su tarea a través de seguimientos, investigación, fotos, etc.; deberá llevar lo recolectado al analista de inteligencia, quien se encargará de graficar lo más claro y precioso lo que le proveen, con el fin de tener clara la investigación y lo objetivos o targets inmersos en ésta.

4.1.5. Cadena de Custodia

La cadena de custodia dentro del delito informático y en especial en Ecuador es un asunto controvertido, pues por un lado porque la evidencia digital en Ecuador es un tema relativamente nuevo, y por otro porque las herramientas forenses para preservación de la información no están del todo actualizadas a los estándares internacionales que hoy por hoy se exigen en laboratorios informático forenses de última tecnología.

La cadena de custodia aplicada a una prueba se define a grosso modo como el procedimiento técnico forense sobre el cual se trata de conservar la integridad física y lógica de una evidencia obtenida de un hecho presumible. Esta conservación va desde la identificación y recolección de la prueba en la escena del crimen, pasando por un registro, hasta su posterior traslado a un lugar seguro para su almacenamiento y un análisis final para ser practicado en la etapa de prueba e incorporado al expediente del proceso como prueba válida.

Para que la cadena de custodia sea considerada válida como tal, se debe seguir un procedimiento forense del tal modo que la prueba se mantenga intacta, de manera que, con herramientas forenses se proceda a hacer una copia exacta de la información en la

que se va a trabajar, esto en el caso de disco duro, pendrive, cd u otro medio magnético que almacene información, a su vez, en el caso de la incautación del material objeto de la infracción, deberá ser éste recolectado en presencia del Fiscal y la Policía Judicial, a fin de verificar que el levantamiento de la evidencia vaya cumpliendo los requisitos de la cadena de custodia, entre los principales requisitos esta que la evidencia vaya metida en bolsas plásticas, en las cuales se fije su fecha de recolección, características del objeto, marca, modelo u otra características en específico.

El perito español Javier Rubio Alamillo señala "*que muchas veces se confunde el término cadena de custodia y se le asocia un significado de no modificación de la prueba. Esto que, en un principio, pudiera parecer lo mismo, realmente no lo es. La conservación de la cadena de custodia siempre implica una no modificación de la prueba, pero una no modificación de la prueba, no implica que se pueda garantizar ante un tribunal que se ha conservado la cadena de custodia*".[60]

El mantenimiento de la cadena de custodia en el peritaje informático es una tarea muy difícil que no siempre puede ser llevada a cabo por determinadas eventualidades y, para que sea aceptada como tal en un proceso judicial, el Fiscal deberá estar presente en el momento de la incautación o intervención del material. Si esto no fuese posible, o si fuese el cliente el que entregó al perito informático una prueba y no se puede garantizar su autenticidad, o si en el transcurso de la pericia la prueba resultó contaminada, es el perito el que, según su leal saber y entender, debe analizar la prueba y elaborar un dictamen indicándole al juez su opinión profesional sobre la misma y sus implicaciones, dejando claro en todo momento que, al no haberse podido conservar la cadena de custodia, siempre existen posibilidades, aunque sean remotas o muy remotas, de modificación maliciosa de esta. "*Para evitar sospechas o suspicacias por parte del juez, siempre se aconseja, aunque no sea posible conservar la cadena de custodia de las pruebas, trabajar sobre copias de las pruebas o, en caso de que sea necesario trabajar sobre los originales, realizar las mencionadas copias, para tener siempre respaldos de cara al informe pericial informático*

[60] RUBIO ALAMILLO, Javier. "Cadena de Custodia en el Peritaje Informático"
Internet: http://peritoinformaticocolegiado.es/cadena-de-custodia-en-el-peritaje-informatico/
Acceso: 01/12/2013

y a que el juez tenga siempre disponible la demostración de la integridad de las pruebas".[61]

4.1.6. Investigación de la Escena del Crimen

La escena del crimen es el punto de inicio de la investigación, donde se busca recabar todas las evidencias posibles a fin de demostrar en un primer lugar, la existencia del delito, y en un segundo lugar, cual o cuales son los supuestos responsables de la infracción. Es deber del Estado asegurar y procurar una adecuada investigación con el fin de garantizar una justicia rápida, oportuna y justa en favor del afectado, cumpliendo de esta manera con la tutela efectiva sobre el bien jurídico perjudicado.

En el manual manejo de evidencias digitales y entornos informáticos de la Fiscalía General del Estado de Ecuador[62], de autoría del profesor Santiago Acurio del Pino, indica que los investigadores forenses tienen ciertas responsabilidades que las deben cumplir a cabalidad para establecer la escena del delito, entre éstas cita las siguientes:

1. **OBSERVE Y ESTABLEZCA LOS PARÁMETROS DE LA ESCENA DEL DELITO**
   Aquí el profesor Acurio del Pino, hace una referencia relacionada al responsable que fija la escena del delito, así este deberá indicar si el delito ya ha sido consumado en su totalidad o se sigue cometiendo. Éste debe de tomar nota de las características físicas del área. Además señala que para los investigadores forenses esta etapa debe ser extendida a todo sistema de información y de red que se encuentre dentro de la escena.

2. **INICIE LAS MEDIDAS DE SEGURIDAD**
   El objetivo principal en toda investigación es mantener la seguridad de los sujetos actuantes de la investigación es decir investigadores y técnicos. Si se observa que dentro de la investigación de la escena del delito se presentan ciertas inconvenientes

[61] RUBIO ALAMILLO, Javier. "Cadena de Custodia en el Peritaje Informático"
Internet: http://peritoinformaticocolegiado.es/cadena-de-custodia-en-el-peritaje-informatico/
Acceso: 01/12/2013
[62] ACURIO DEL PINO, Santiago. "Manual de manejo de evidencias digitales y entornos informáticos".
Internet: http://www.oas.org/juridico/english/cyb_pan_manual.pdf
Acceso: 05-09-2013

problemas o amenazas, lo más prudente en neutralizar o mitigar el problema, de manera que los sujetos actuantes puedan trabajar con seguridad y confianza en la investigación del delito.

3. ASEGURE FÍSICAMENTE LA ESCENA

Es importar que se deba retirar a toda persona o agente externo que pueda estar merodeando la escena del delito, para prevenir la contaminación de la evidencia o su posible alteración.

4. ASEGURE FÍSICAMENTE LAS EVIDENCIAS

"Este paso es muy importante a fin de mantener la cadena de custodia[63] *de las evidencias, se debe guardar y etiquetar cada una de las evidencias. En este caso se aplican los principios y la metodología correspondiente a la recolección de evidencias de una forma práctica. Esta recolección debe ser realizada por personal entrenado en manejar, guardar y etiquetar evidencias"*[64].

5. ENTREGAR LA ESCENA DEL DELITO

Después de que se han cumplido todas las etapas anteriores, la escena puede ser entregada a las autoridades que se harán cargo de la misma. Esta situación será diferente en cada caso. Lo esencial de esta etapa es verificar que todas las evidencias del caso se hayan recogido y almacenado de forma correcta.

---

[63] CADENA DE CUSTODIA: La cadena de custodia es un sistema de aseguramiento que, basado en el principio de la "mismidad", tiene como f in garantizar la autenticidad de la evidencia que se utilizará como "prueba" dentro del proceso. La información mínima que se maneja en la cadena de custodia, para un caso específico, es la siguiente: a) Una hoja de ruta, en donde se anotan los datos principales sobre descripción de la evidencia, fechas, horas, custodios, identificaciones, cargos y firmas de quien recibe y quien entrega; b) Recibos personales que guarda cada custodio y donde están datos similares a los de la hoja de ruta; c) Rótulos que van pegados a los envases de las evidencias, por ejemplo a las bolsas plásticas, sobres de papel, sobres de Manila, frascos, cajas de cartón, etc.; d) Etiquetas que tienen la misma información que los rótulos, pero van atadas con una cuerdita a bolsas de papel kraft, o a frascos o a cajas de cartón o a sacos de fibra; e) Libros de registro de entradas y salidas, o cualquier otro sistema informático que se deben llevar en los laboratorios de análisis y en los despachos de los f iscales e investigadores.

[64] ACURIO DEL PINO, Santiago. "Manual de manejo de evidencias digitales y entornos informáticos".
Internet: http://www.oas.org/juridico/english/cyb_pan_manual.pdf
Acceso: 05-09-2013

6. ELABORAR LA DOCUMENTACIÓN DE LA EXPLOTACIÓN DE LA ESCENA

"Es Indispensable para los investigadores documentar cada una de las etapas de este proceso, a fin de tener una completa bitácora de los hechos sucedidos durante la explotación de la escena del delito, las evidencias encontradas y su posible relación con los sospechosos. Un investigador puede encontrar buenas referencias sobre los hechos ocurridos en las notas recopiladas en la explotación de la escena del Delito".[65]

4.1.7. Elementos de convicción y punibilidad

Para ser punible un acto se necesita de elementos de convicción llamados también en investigación forense elementos de prueba digital. Los elementos de convicción son el conjunto de pruebas en el caso de delitos informáticos electrónicas o digitales necesarias para probar la materialidad del delito, sin las cuales fuese imposible delimitar el delito e imponer una pena por este. Estas pruebas deberán ser mostradas como fidedignas al momento de su práctica en la audiencia además de estar acompañadas del respectivo informe pericial realizado por un perito calificado. Para que esta pericia o experticia sea válida debe ser realizada por peritos avalados por el Consejo Nacional de la Judicatura o peritos privados según lo señala los artículos 11 y 12 del Reglamento sustitutivo para la acreditación de peritos del año 2009.

Es importante mencionar que al hablar sobre precisar y fijar elementos de convicción determinados en relación a los delitos informáticos es algo difícil, pues para cada caso hay un hecho distinto y más cuando se los da a través de medios virtuales y electrónicos, inclusive porque el asimilar o desconocer cada modus operandi con que el atacante ha actuado se vuelve un tormento para el desconocedor del tema, es así que lo elementos encontrados y utilizadas en el proceso como material de la infracción, deberán ser analizados y entendidos por las partes procesales, de modo que el proceso sea claro, conciso y neutral para éstas, sin que pueda afectar de manera alguna el interés que se da en el proceso penal y el resultado deseado en busca de justicia.

---

[65] ACURIO DEL PINO, Santiago. "Manual de manejo de evidencias digitales y entornos informáticos".
Internet: http://www.oas.org/juridico/english/cyb_pan_manual.pdf
Acceso: 05-09-2013

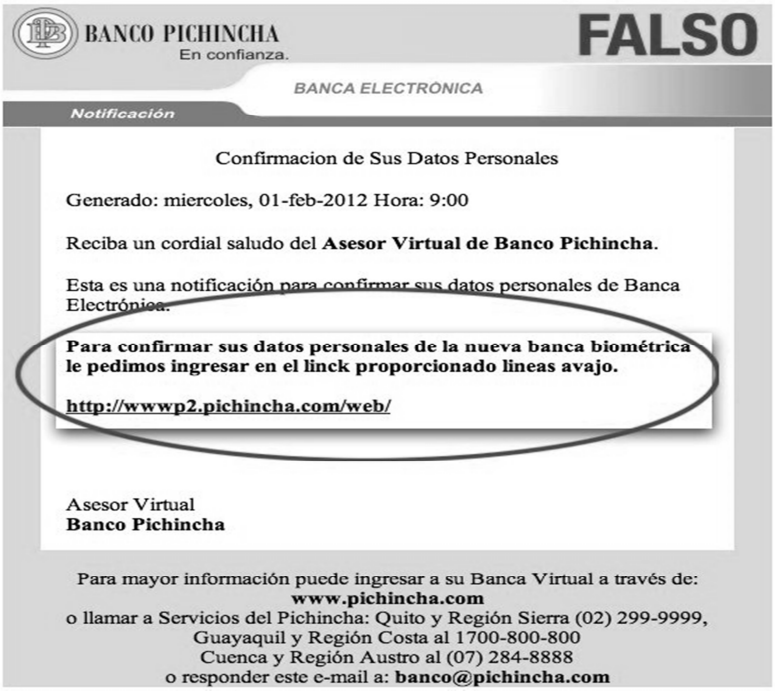
CAPITULO V
CASOS EN ECUADOR

5.1. Desvío y hurto de dinero, Caso Emetel 1996

Este delito trata sobre el redondeo que se realizaba en las planillas realizadas por el antiguo EMETEL, y que no se sabía a donde se dirigían estas cantidades que muchas veces eran demasiado pequeñas para que cause discusión, pero ya en grandes cantidades era una cantidad de dinero muy apreciable, para este tipo de delito informático se utilizó la técnica del Salami o Rounding Down.

5.2. Ataques de Phishing y Carding a bancos ecuatorianos

Entre los años 2009 a 2012 se dio una época de continuo auge de delitos informáticos en el ámbito bancario siendo perjudicados cientos de usuarios; el delito más común que se cometía era el de transferencias electrónicas sin autorización, para que se cometa este tipo de ilícito el ciberdelincuente creaba una página idéntica a la original (llamada en el mundo del hacking “Scam”) en la que posteriormente a través de una técnica llamada “ingeniería social”, hacían creer al usuario que estaba entrando a un sitio bancario real y seguro, que en la realidad no lo era, donde posteriormente ingresaba su información como username, passwords y e-keys que después facilitarían al ciberdelincuente el cometer el delito. Entre los bancos más afectados se encontraban el Banco del Pichincha, Banco de Guayaquil, Banco Amazonas, Banco Proamérica, entre otros.



[66]

Banco Amazonas (Av. Amazonas y Villalengua) ATM65

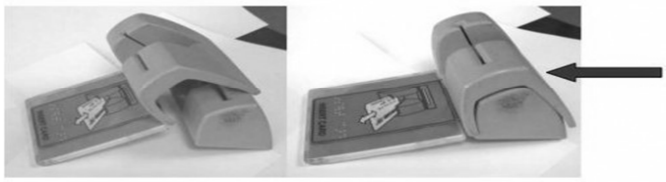
Dentro de lo que son delitos informáticos a tarjetas de crédito, uno de los cajeros automáticos más afectados a nivel nacional fue el ATM N°65 ubicado en la Av. Amazonas y Villalengua a exteriores del Banco Amazonas. Para dicho delito los ciberdelincuentes instalaron un aparato electrónico llamado “skimmer” por encima del lector original de tarjetas de crédito y débito, aparato que al ser instalado y funcionando copiaba todos los datos de una tarjeta bancaria a un chip muy parecido al de un celular, donde al final del día almacenada información de decenas de usuarios para la posterior duplicación de estas tarjetas de crédito, estas tarjetas duplicadas se las utilizaba con fines comerciales como compras por internet y con fines lucrativos para poder retirar dinero de otros cajeros como si fuese la original.

[66] Imagen de una carta o letter donde se indica un mensaje en el cual el cliente debe confirmar sus datos personales, una técnica típica utilizada por los ciberdelincuentes para sus atracos, en la parte inferior de la misma imagen se indica un link que al momento de hacer clic redirige a un sitio idéntico al original donde posteriormente se hurtarán los datos del usuario. Tómese en cuenta que en muchos de los casos quiénes cometen estos ilícitos no tienen buena ortografía lo que da como indicio de que el mensaje es fraudulento, fijarse en imagen.

Hasta diciembre del año 2011, se presentaron 140 denuncias de tarjetas clonadas a través de este cajero, de las investigaciones hechas se dio a conocer que los autores era un banda de crimen organizado compuesta por ciudadanos colombianos y peruanos.

[67]

The real card reader slot. The capture device


The side cut out is not visible when on the ATM.
[68]

[69]

[67] Skimmer para la obtención de datos de la banda magnética de una tarjeta de crédito.
[68] Proceso de colocación de un Skimmer encima de una lectora de tarjetas magnéticas.
[69] Colocación del Skimmer en el ATM (cajero automático)

5.3. Terrorismo informático, Caso Anonymous 2010

Anonymous Ecuador – #opcondorlibre (2011): En agosto del 2011 un pseudo grupo derivado de Anonymous llamado Anonymous Ecuador planeó ataques informáticos a sitios gubernamentales por motivo del proyecto de la Ley Orgánica de Comunicación que en su art.10 señalaba "*quién difunda por cualquier medio o plataforma tecnológica que denote el uso intencional de la fuerza física, o psicológica, de obra o de palabra contra uno mismo, contra cualquier otra persona, grupo o comunidad, así como en contra de los seres vivos y la naturaleza, tanto en contextos reales, ficticios o fantásticos"*.

Para los ataques perpetuados se tomó como fecha el 10 de agosto, ya que al ser esta fecha cívica nacional por el Día de la Independencia, fue ocasión para promocionar una independencia de los medios de comunicación en contra de un gobierno autoritarista.

Qué es Anonymous?

Anonymous data del año 2003 formado inicialmente en EE-UU, el nombre de *Anonymous* en sí mismo está inspirado en el anonimato que perciben los usuarios cuando publican comentarios e imágenes en Internet. El uso del término es el sentido de una identidad compartida, y también de la película V de Venganza. Las definiciones de Anonymous tienden a enfatizar el hecho de que el término no puede ser fácilmente comprendido por una descripción simple, y en su lugar es descrita por cualidades percibidas.

Estructura de Anonymous

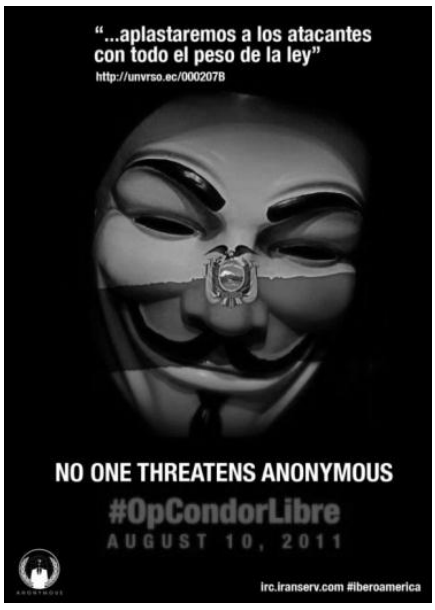
Anonymous se caracteriza por no tener "cara", líderes, ni institución. Anonymous está conformado por personas de todo el mundo, todas las edades, religiones y profesiones.

Motivaciones

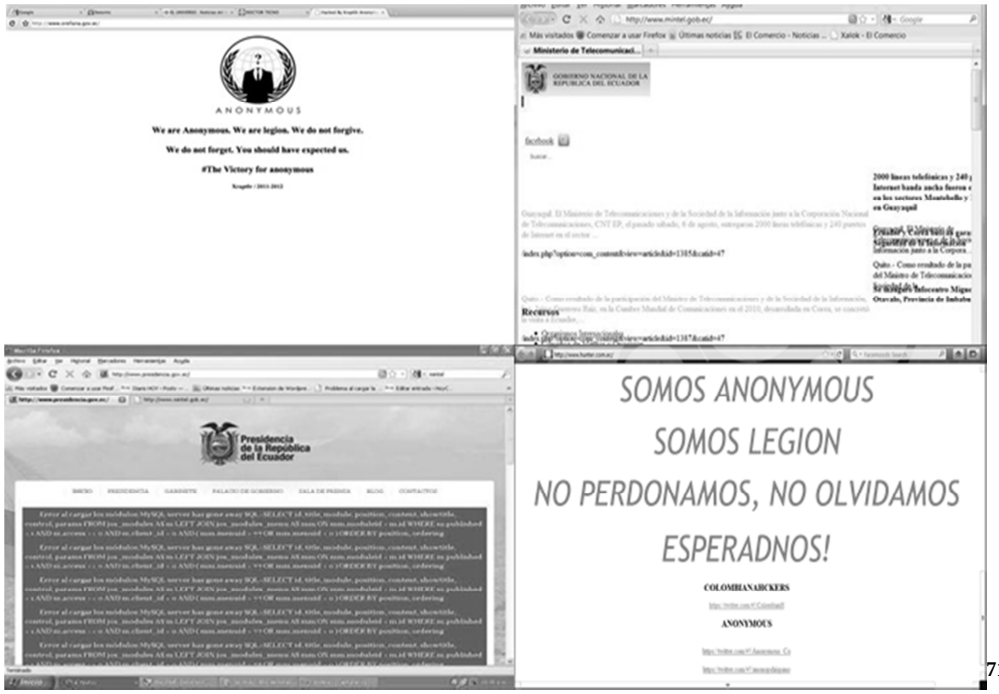
La máscara que usan hace referencia al personaje que sale en la película "V de Vendetta", un tipo revolucionario y anarquista que van en contra de todas las reglas.

Expansión

La célula de Anonymous primordialmente se formó en EE-UU, pero al ser ahí un país de habla inglesa, decidieron personas de habla hispana formar Anonymous en varios países como Colombia, México, Argentina, España, Perú y al ver la unión de varios países se hizo Anonymous Iberoamérica.



[70] Afiche de la Operación "Cóndor Libre" por parte de Anonymous Ecuador, 10 de Agosto del 2011



[71]

Como actúa Anonymous

Anonymous actúa de manera anónima alrededor de todo el mundo, contra grupos o personas que atentan contra la ciudadanía en casos de diferente índole. *(Ejemplo: Pedofilia, trata de blancas, narcotráfico, etc.)*

Modus operandi para protección de ataques

El modo de actuar de los miembros de Anonymous para no ser rastreados:

1. Si los ataques lo van a hacer fuera de su casa recurrir a un cyber.
2. Si los ataques los van a hacer desde su pc o laptop personal descargan ciertos programas gratuitos o de pago que lo que hacen es cambiar su IP o esconderla, estos programas pueden ser:

-Proxy: Un proxy, en una red informática, es un programa o dispositivo que realiza una acción en representación de otro.

[71] Ataques de Anonymous a varios sitios web en Ecuador en el año 2011.

-Tor: Programa que esconde la IP y reemplaza por otra IP de un país extranjero.

-VPN Virtual Private Network: Igualmente reemplaza o esconde la IP por la de otro país. Entre las principales las podemos encontrar en los siguientes sitios:

-http://cyberghostvpn.com
-http://hotspotshield.com
-http://proxpn.com
-https://anonymityonline.org

Su llegada a ecuador

La llegada de Anonymous a Ecuador se dio a mediados de Julio de ese año a causa de la Ley Orgánica de Comunicación en la que en su art.10 señala lo siguiente: *"Quién difunda por cualquier medio o plataforma tecnológica que denote el uso intencional de la fuerza física, o psicológica, de obra o de palabra contra uno mismo, contra cualquier otra persona, grupo o comunidad, así como en contra de los seres vivos y la naturaleza, tanto en contextos reales, ficticios o fantásticos"*

Operación Cóndor Libre

COMUNICADO

Saludos ciudadanos del mundo, Somos Anonymous.

Como respuesta a la reciente injusticia AL DIARIO EL UNIVERSO, hemos decidido iniciar la #OpCondorLibre con el fin de luchar contra la censura a los medios informativos de nuestro país.

El Presidente RAFAEL CORREA recientemente ha tomado posturas radicales en contra de la libertad de expresión del pueblo y los medios de comunicación, EL CUAL ANONYMOUS NO ACEPTARÁ.

Días atrás, el gobierno ecuatoriano inició actividades en contra de los medios de comunicación que tuvieran diferencias ideológicas frente a sus políticas; Anteriormente el gobierno se había apoderado de diversos medios de comunicación, controlando canales de televisión, como: TC Televisión, Gama Tv, Cn3, las radios Carrusel, Súper k-800, y el periódico conocido como El Telégrafo, ayudándose así mismo en el poder.

Estos medios continúan en manos de Rafael Correa, siendo a su vez portador de su palabra, ocultando la corrupción de su gobierno y evitando que los ciudadanos conozcan la verdad del país.

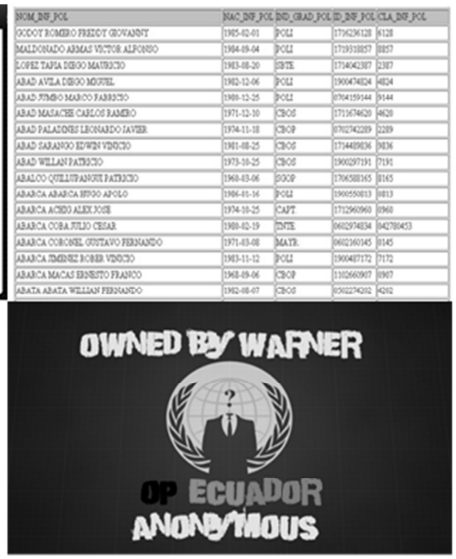
Los escasos medios de comunicación que continúan en la lucha por la libertad de expresión están siendo censurados, atacados y difamados por el gobierno, Desacreditándolos por el hecho de exponer una verdad que no está acorde con las políticas de estado. [72]

[72] Comunicado de Anonymous al Gobierno de Ecuador

Diferencia entre hacktivismo y ciberactivismo

Un Hacktivista es aquel que usa medios digitales legales o ilegales para realizar actos de protesta política no violentos, sobre todo relacionados con el libre acceso a la información, una especie de desobediencia civil a través de la red. Los actos más conocidos que Anonymous realiza a este respecto son los ataques de denegación de servicio DoS, o más sofisticado, el DDoS, que es una ataque de denegación de servicio coordinado. [73]

En cambio el Ciberactivismo difiere del Hacktivismo en que no usan métodos ilegales. Entendiéndose como ello acciones de activismo a través de la red sin comprometer o alterar el normal funcionamiento de otras empresas, organizaciones o actividades. [74] Es aconsejable y necesario conceptualizar cada término para evitar cometer errores al momento de su interpretación.



75

[73] MAESTRE, Antonio. "Anonymous: Ciberactivismo, Hacktivismo o Delincuencia" Internet: http://www.prnoticias.com/index.php/internet-y-redes-sociales/553-internet/20108904-anonymous-ciberactivismo-hacktivismo-o-delincuencia
Acceso: 05/08/2012

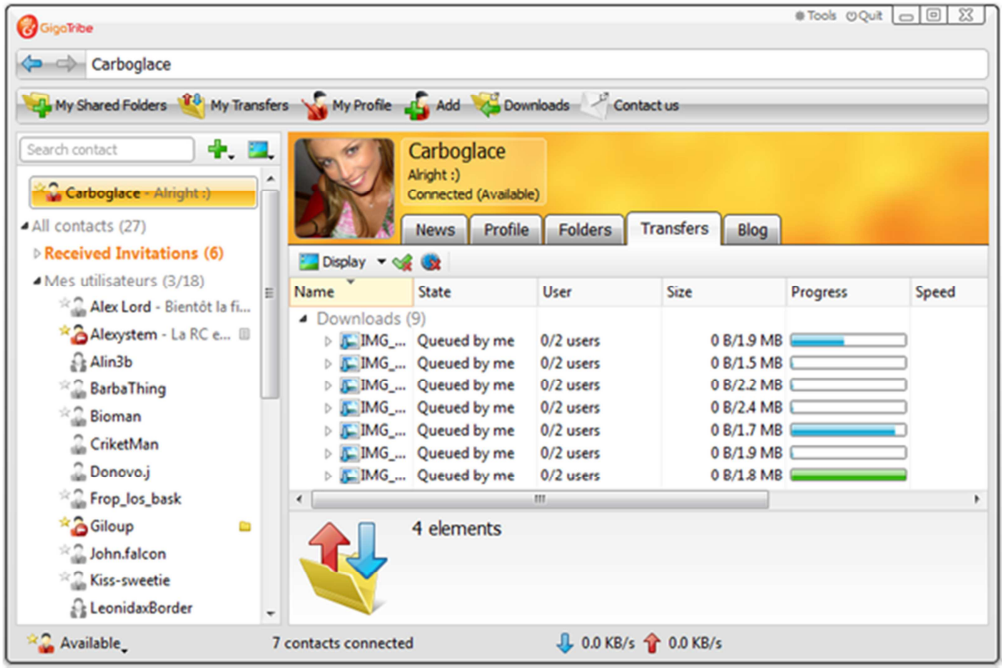
[74] Ídem

[75] Ataque a páginas gubernamentales y empresariales en el Ecuador

5.4. Pedofilia y crimen organizado, Caso Gigatribe 2010

Gigatribe – Pornografía infantil (2011) +200GB entre videos y fotos: GigaTribe es una red peer-to-peer para intercambio de archivos. Originalmente desarrollada en Francia, su versión fue lanzada en noviembre de 2008. Ofrece una versión gratis y otra de pago; con la versión de pago los usuarios pueden restringir el acceso a sus archivos encriptados a un grupo de amigos de confianza.[76]

En 2010, un juez federal de Estados Unidos dictaminó que la expectativa razonable de privacidad no se extiende al intercambio de archivos en GigaTribe. En el caso, un informante le dio a la policía acceso a los archivos de sus amigos en GigaTribe, y se descubrió pornografía infantil.[77]



[76] REISINGER, Don. "GigaTribe brings private P2P sharing to U.S"
Internet: http://www.cnet.com/news/gigatribe-brings-private-p2p-sharing-to-u-s
Acceso: 17-11-2012
[77] BRENNER, Susan. "Gigatribe and the 4th Amendment"
Internet: http://cyb3rcrim3.blogspot.com/2010/06/gigatribe-and-4th-amendment.html
Acceso: 25-06-2012

En noviembre del 2011 se descubrió una cuenta de Gigatribe que contenía 300 gigabytes de pornografía infantil, la denuncia de dicha cuenta comenzó en Australia, en donde la policía en su investigación dio a conocer que la direcciones IP's de donde se habían subido dichas imágenes provenían de Ecuador, luego de indicado eso y al ser delito transnacional la Interpol como organización internacional, remitió los documentos investigados en Australia a la Interpol de Melbourne en dicho país para su posterior envío a la Interpol de Lyon en Francia, luego Interpol de Londrés en Reino Unido para su posterior traslado a la Interpol de Buenos Aires en Argentina la misma que haría llegar a la Interpol de Quito en Ecuador. Una vez con los documentos en Ecuador la Fiscalía General del Estado junto a Interpol, DGI y Policía Nacional prosiguieron con las investigaciones dando como resultado final la localización de los autores del ilícito los mismos que se encontraban en la ciudad de Guayaquil.

5.5. Ciberespionaje y filtración de información, Caso Wikileaks

En el 2011, la organización mundial Wikileaks encabezada por Julian Assange había filtrado cables diplomáticos de la Embajada de Estados Unidos en Quito, en dichos cables se hacían aseveraciones de corrupción de miembros en el interior de la Policía Nacional. En estos cables también se indicó el apoyo por parte de los EE-UU a políticos y banqueros ecuatorianos que se encontraban en contra del gobierno del Presidente del Ecuador, Ec.Rafael Correa Delgado.

Luego de que el gobierno de Ecuador se enterara de dichos cables se cerró momentáneamente las relaciones diplomáticas con EE-UU, siendo así el Canciller Raúl Patiño, pidió de forma inmediata el abandono del país de la embajadora Heather Hodges a quien la declararon como persona no grata en Ecuador.

5.6. Robo de información, Casos hackeo de redes sociales y correo electrónico entre 2006-2014

Diariamente se cometen ataques a websites no solo ecuatorianas sino a nivel mundial, algunos de estos ataques son hechos por ecuatorianos, personas aficionadas a la

tecnología e informática las cuales penetran sitios con el propósito de dejar su marca personal es decir un signo o huella que dé a entender que ellos estuvieron ahí.

Ciertamente en Ecuador hay personas con el talento suficiente para emplear este conocimiento como beneficio para el país, más no lo hacen, esto es porque según ellos y por entrevistas realizadas, no hay el incentivo tanto pecuniario como laboral para que ellos se puedan dedicar a estas labores con el fin de proteger al sistema informático gubernamental ecuatoriano.

En el territorio ecuatoriano, los ataques a páginas web suelen se hechos a través de la técnica del "Defacing" antes ya mencionada en esta disertación. De los grupos conocidos en Ecuador de hacking podemos destacar a: Ecuadorian Hacking Team, Kalimndor Team, Fenix Hackers, AnonAzules, AnonEcuador, Latin Hack Team y otros de menor importancia.

78

[78] Ataque web mediante la técnica del Defacement a uno de los subdominios de la página web de la PUCE.

CONCLUSIONES Y RECOMENDACIONES

Dentro del paradigma que envuelve a los delitos informáticos en el Ecuador hay un gran problema, por lo que se deben tomar vías, medidas y formas para solventar y solucionar estos ilícitos, en principio los delitos informáticos quedan impunes por motivo de desconocimiento de Fiscales y Jueces del tema, que al momento de dictaminar y juzgar no tienen una idea clara sobre la materia penal informática y los elementos que la componen, además que en ciertos casos no aplican el tipo penal correspondiente para juzgar un delito determinado, no lo encuentran porque la confusión sobre delitos informáticos en los servidores judiciales y administradores de justicia en grande, con la llegada y vigencia del Código Orgánico Penal Integral tenemos inclusive más tipos penales que en el Código Penal ya derogado, para juzgar casos en relación a delitos informáticos, pero el problema no se halla en que tengamos los tipos penales, si no que se pueda adecuar correctamente el tipo al delito suscitado, para esto no sólo se necesita conocimiento de la ley, sino también de la doctrina referente a esta, entiéndase como conocimiento básico y previo de los diferentes tipos penales incorporados en el Código Penal, ahora llamado COIP.

A criterio personal, en primer lugar en el Ecuador se debe crear un cultura tecnológica, en la cual a las generaciones anteriores y nuevas generaciones de ciudadanos se les guíe y eduque sobre los mecanismos de protección para evitar ser víctimas de fraudes y delitos informáticos; en segundo lugar se debería dar prioridad a estos delitos tipificándolos de una forma adecuada y ordenada, si bien ya se tiene en la

legislación varios de estos tipificados, falta un reglamento en donde se dé alcance al espíritu de la norma, de manera que pueda ser entendida no sólo por jueces, fiscales y abogados, sino por la ciudadanía en general; y cómo último punto, se deberían priorizar dando puestos de trabajo a personas con la capacidad intelectual y técnico en lo referente a seguridad informática, inteligencia cibernética y análisis de información sensible, ya que estas personas en futuro serán las encargadas de proteger todo el sistema integral y tecnológico del estado ecuatoriano, además de brindar e implementar la seguridad necesaria en casos de espionaje cibernético que puedan evitar la fuga de información sensible que afecte a la seguridad del Estado como bien jurídico protegido.

****

BIBLIOGRAFÍA

- **ACURIO DEL PINO, Santiago.** *Derecho y Nuevas Tecnologías.* Quito, Corporación de Estudios y Publicaciones, 1ª Edición, 2010.
- **CORPORACIÓN DE ESTUDIOS Y PUBLICACIONES.** *Código Penal ecuatoriano.* Quito, Corporación de Estudios y Publicaciones, Edición Marzo, 2009.
- **CORPORACIÓN DE ESTUDIOS Y PUBLICACIONES.** *Código Civil ecuatoriano.* Quito, Corporación de Estudios y Publicaciones, Edición Septiembre, 2010.
- **CORPORACIÓN DE ESTUDIOS Y PUBLICACIONES.** *Código Civil ecuatoriano.* Quito, Corporación de Estudios y Publicaciones, Edición Octubre, 2011.
- **CORPORACIÓN DE ESTUDIOS Y PUBLICACIONES.** *Código Orgánico Integral Penal.* Quito, Corporación de Estudios y Publicaciones, 1ª Edición, 2014.
- **DIARIO EL HOY.** Archivo Histórico. *"Página web del Municipio de Quito destruida por crackers"*. Quito, Editorial El Hoy. Fecha: 06-02-2001.
- **FISCALÍA GENERAL DEL ESTADO DE ECUADOR,** Dirección de Gestión Procesal Penal – SINAEP. "Reporte de Delitos Informáticos 2009 – 2013".
- **LEIVA JIJENA, Renato.** *Chile, la protección penal de la intimidad y el delito informático.* Santiago de Chile, Editorial Andrés Bello, 2ª Edición, 1992.
- **MÁRQUEZ ESCOBAR, Carlos.** *El Delito Informático*. Bogotá, Editorial Leyer, 1ª Edición, 2014.
- **MUNICIPIO DE QUITO.** Boletín de Prensa. *"Hackers destruyen página web del Municipio de Quito"*. Quito, Fecha: 06-02-2001.
- **REGISTRO OFICIAL.** "Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos". Suplemento Oficial N° 557 del 17 de Abril del 2002.
- **SACOTO DE MERLYN, Pilar.** *Apuntes de Introducción al Derecho Penal*. Citada por el Autor.
- **TELLÉZ VALDÉS, Julio.** *Derecho Informático.* México D.F, Editorial Mc Graw Hill, 4ª Edición, 2006.

NETGRAFÍA

- **ACURIO DEL PINO, Santiago.** "Manual de manejo de evidencias digitales y entornos informáticos".
  Internet: http://www.oas.org/juridico/english/cyb_pan_manual.pdf
  Acceso: 05-09-2013
- **BRENNER, Susan.** "Gigatribe and the 4th Amendment"
  Internet: http://cyb3rcrim3.blogspot.com/2010/06/gigatribe-and-4th-amendment.html
  Acceso: 25-06-2012
- **CALLEGARI, Nidia.** Citado por: CONDE O'DONNELL, Hugo. "El Delito Informático". Internet:
  http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf
  Acceso: 07/06/2013
- **COUNCIL OF EUROPE.** "Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse".
  Internet: http://conventions.coe.int
  Acceso: 20-03-12
- **DE LA LUZ LIMA, María.** Citado por: CONDE O'DONNELL, Hugo. "El Delito Informático".
  Internet:www.dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf
  Acceso: 07/06/2013
- **EUROLEX.** "Council Framework Decision on combating the sexual exploitation of children and child pornography".
  Internet: http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_013/l_01320040120en00440048.pdf
  Acceso: 20-03-12

- **INFORMÁTICA FORENSE COLOMBIA.** "Terrorismo virtual" Internet:www.informaticaforense.com.co/index.php?option=com_content&view=article&id=88&Itemid=90 Acceso: 15-04-2012
- **INTERNATIONAL TELECOMUNICATION UNION.** *Global Cybersecurity Agenda / High-Level Experts Group, Global Strategic Report.* Ginebra, UN ITU, 1ª Edición, 2008. Página 30. Internet: www.itu.int/osg/csd/cybersecurity/gca/global_strategic_report/index.html. Acceso: 20-01-2011
- **INTERNATIONAL TELECOMUNICATION UNION.** *El ciberdelito: Guía para los países en desarrollo.* Ginebra, UN ITU, 1ª Edición, 2008. Página 28. Internet: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf Acceso: 05-04-2011
- **LEVENE, Ricardo y CHIARAVALLORTI, Alicia.** "Introducción a los Delitos Informáticos, tipos y legislación" Internet: http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml Acceso: 01/12/2013
- **RECOVERY LABS.** "Definición de Delito Informático" Internet: http://delitosinformaticos.info/delitos_informaticos/definicion.html Acceso: 12/07/2012
- **REISINGER, Don.** "GigaTribe brings private P2P sharing to U.S" Internet: http://www.cnet.com/news/gigatribe-brings-private-p2p-sharing-to-u-s Acceso: 17-11-2012
- **REVELO, Héctor.** "Estadísticas 2010, Delitos Informáticos en el Ecuador." Internet: http://www.abogados.ec/2011/02/estadisticas-2010-delitos-informaticos-en-ecuador/ Acceso: 02/05/2012
- **RUBIO ALAMILLO, Javier.** "Cadena de Custodia en el Peritaje Informático" Internet: http://peritoinformaticocolegiado.es/cadena-de-custodia-en-el-peritaje-informatico/ Acceso: 01/12/2013

- **SÁENZ, Ricardo.** "Reforma del Código Penal Argentino"
  Internet: http://delitosinformaticos.fiscalias.gob.ar/actualidad/reforma-del-codigo-penal/
  Acceso: 17/03/2014
- **SARZANA, Carlos.** Citado por: CONDE O'DONNELL, Hugo. "El Delito Informático". Internet:
  http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf
  Acceso: 07/06/2013
- **TÉLLEZ VALDÉS, Julio.** Citado por: LEVENE, Ricardo y CHIARAVALLORTI, Alicia. "Introducción a los Delitos Informáticos, tipos y legislación"
  Internet: http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml
  Acceso: 01/12/2013
- **UNITED NATIONS.** "United Nations Convention of Right of the child.
  Internet: http://www.hrweb.org/legal/child.html.
  Acceso: 19-03-12
- **UNIVERSIDAD DE SALAMANCA.** "Qué es un perito informático?".
  Internet: http://diarium.usal.es/salamandra/informatica/%C2%BFque-es-un-perito-informatico/
  Acceso: 05-09-2013
- **UNIVERSIDAD NACIONAL DE MÉXICO, Departamento de Investigación.** Citado por: VIEGA RODRÍGUEZ, María José. "Un nuevo desafío jurídico: los Delitos Informáticos". Internet: http://mjv.viegasociados.com/wp-content/uploads/2011/05/DelitosInformaticos.pdf
  Acceso: 05/01/2014
- **WOLAK FINKELHOR, Mitchell.** "Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study"
  Internet: http://www.missingkids.com/en_US/publications/NC144.pdf
  Acceso: 20-02-2013

GLOSARIO

Amenaza: Situación o evento que puede provocar daños en un sistema.
Anonimato, anonimia: Carácter o condición de anónimo (desconocimiento del nombre o identidad).
Aplicación engañosa: Aplicación cuya apariencia y comportamiento emulan a una aplicación real. Normalmente se utiliza para monitorizar acciones realizadas por atacantes o intrusos.
Autenticación, autentificación: Proceso de confirmar la identidad de una entidad de sistema (un usuario, un proceso, etc.).
Bug, Hole: Agujero. Se trata de un defecto en el software normalmente el S.O y aplicaciones web que permite la intrusión de los hackers.
Autorización: Acción de otorgar el acceso a usuarios, objetos o procesos.
Caballo de Troya, troyano: Programa informático de aspecto inofensivo que oculta en su interior un código que permite abrir una "puerta trasera" en el sistema en que se ejecuta.
Capa de Conexión Segura (SSL): Protocolo creado por Netscape para permitir la transmisión cifrada y segura de información a través de la red.
Carder: Persona que se encarga de la duplicación y uso de tarjetas de crédito
Cifrado: Proceso mediante el cual se toma un mensaje en claro, se le aplica una función matemática, y se obtiene un mensaje codificado.
Código abierto: Software que cumple los criterios descritos por la iniciativa "Open Source". Este término no implica el acceso al código fuente.
Confianza: Esperanza firme de que un sistema se comporte como corresponde.
Confidencialidad: Requisito de seguridad que indica que el acceso a los recursos de sistema debe estar limitado exclusivamente a los usuarios con acceso autorizado.
Cracker: Individuo que se dedica a eliminar las protecciones lógicas y físicas del software. Normalmente muy ligado al pirata informática.
Defacement: Es desconfigurar una página en su totalidad subiendo un mensaje y una imagen al index del sitio que fue vulnerado.

Denegación de servicio (DoS): Estrategia de ataque que consiste en saturar de información a la víctima con información inútil para detener los servicios que ofrece.

Denegación de servicio distribuida (DDoS): Estrategia de ataque que coordina la acción de múltiples sistemas para saturar a la víctima con información inútil para detener los servicios que ofrece. Los sistemas utilizados para el ataque suelen haber sido previamente comprometidos, pasando a ser controlados por el atacante mediante un cliente DDoS.

Escáner o analizador de vulnerabilidades: Herramienta diseñada para llevar a cabo análisis de vulnerabilidades.

Falseamiento, enmascaramiento: Modificación de la identidad de origen real durante una comunicación. El método más común consiste en alterar directamente la dirección origen de cada paquete datos.

Gusano: Programa informático que se auto-duplica y auto-propaga. A diferencia que los virus, suelen estar diseñados para redes.

Hacking: Es el entrar de forma ilegal y sin el consentimiento del propietario en su sistema informático para obtener información. No conlleva la destrucción de datos ni la instalación de virus. También lo podríamos definir como cualquier acción encaminada a conseguir la intrusión en un sistema (ingeniería social, caballos de Troya, etc.)

Hacker: Cualquier persona que se dedica a hacer hacking siendo bastante buena con los ordenadores.

IP: IP es la sigla de Internet Protocol o, en nuestro idioma, Protocolo de Internet. Se trata de un estándar que se emplea para el envío y recepción de información mediante una red que reúne paquetes conmutados.

IRC: Inter Relay Chat, es un programa nativo por el cual se comunican muchas redes anónimas de ciberdelincuentes.

Keylogger: Programa o dispositivo que instalado en un computador capta las pulsaciones del teclado, además que capta cada cierto tiempo las interacciones de pantalla que hace el usuario para su posterior remisión a un FTP o e-mail.

Letter: También conocido como Hoax o Bulo es un documento electrónico que simula ser uno verdadero con el propósito de engañar a las personas.

LOIC: Programa para hacer un ataque DoS.

Newbie o Noob: Principiante en el mundo del hacking.

Parche: En seguridad informática, código que corrige un fallo (agujero) de seguridad.

Phreaker: Es el especialista en telefonía (Cracker de teléfono).Un Phreaker posee conocimientos profundos de los sistemas de telefonía, tanto terrestres como móviles.

Pirata informático: Es un delincuente informático que se dedica a la copia y distribución de software ilegal. Este software puede ser comercial crackeado o shareware registrado. También es otro nombre que reciben los crackers, no confundir con los hackers.

Privilegio: Nivel de confianza perteneciente a un objeto de sistema.

Probar mediante explotación: Método de comprobación de seguridad que consiste en lanzar ataques conocidos contra el objetivo y estudiar los resultados. Véase también ("análisis de vulnerabilidades").

Proxy: Es un programa que esconde o suplanta la dirección IP de un equipo.

Procesamiento por lotes, procesamiento en lotes: Procesamiento realizado en intervalos de tiempo, de forma discontinua.

Procesos de confianza: Procesos que sirven para cumplir un objetivo de seguridad.

Protocolo de Control de Transmisión / Protocolo Internet (TCP/IP): Conjunto de protocolos básico sobre los que se fundamenta Internet. Se sitúan en torno al nivel tres y cuatro del modelo OSI.

Protocolo de Tiempo de Red (NTP): Protocolo situado sobre TCP/IP diseñado para permitir la sincronización de los relojes de las máquinas conectadas a través de una red.

Protocolo de Transferencia de Ficheros (FTP): Protocolo que permite a un usuario de un sistema acceder a otro sistema de una red, e intercambiar información con el mismo.

Protocolo de Transferencia de Hipertexto (HTTP): Protocolo usado para la transferencia de documentos WWW.

Puerta trasera: Mecanismo que permite a un atacante entrar y controlar un sistema de forma oculta. Suelen instalarse justo después de comprometer un sistema.

Red Privada Virtual (VPN): Red generalmente construida sobre infraestructura pública, que utiliza métodos de cifrado y otros mecanismos de seguridad para proteger el acceso y la privacidad de sus comunicaciones.

Scam: La duplicación idéntica de un sitio web.

Sistema de Nombres de Dominio (DNS): Servicio distribuido de búsqueda de datos que realiza traducciones entre direcciones IP y nombres de máquinas. La estructura de los nombres

de máquina (nombres de dominio), que son más fáciles de recordar que las direcciones IP, sigue una estructura jerárquica.

Spam: También conocido como correo basura, es aquel que lo envía en forma simultánea o en cadena.

Software libre: Código que otorga libertad a los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el mismo. Véase también ("código abierto").

Vulnerabilidades: Debilidades en un sistema que pueden ser utilizadas para violar las políticas de seguridad.

Virus: Programa informático que tiene como propósito dañar o afectar un sistema.

TABLA COMPARATIVA DELITOS INFORMÁTICOS CODIGO PENAL Y CÓDIGO ORGÁNICO INTEGRAL PENAL

La tabla comparativa hace referencia a los tipos penales informáticos similares, tipificados tanto en el Código Penal como en el Código Orgánico Integral Penal.

S.A: Sujeto Activo
V.R: Verbo Rector
C.P. Código Penal
S.P: Sujeto Pasivo
O.J.P: Objeto Jurídico Protegido
COIP: Código Orgánico Integral Penal

DELITO	Contra la Información Protegida	Obtención y utilización no autorizada de información	Destrucción Maliciosa de Documentos	Falsificación electrónica
ARTÍCULO C.P.	Art.202.1	Art.202.2	Art.262	Art.353.1
ARTÍCULO COIP	Art.229, 233	Art.230	Art.211	Art.306
S.A	Hacker	Delincuente Informático	Funcionario Público	Delincuente Informático
S.P	Agraviado, perjudicado: Estado o sector privado	Agraviado, perjudicado: Dueño de la información	Agraviado, perjudicado: Estado	Agraviado, perjudicado: Ciudadanía y el Estado
V.R	Violentar clases o sistemas de seguridad	Obtener información	Destrucción y supresión de documentos	Alterar o modificar mensajes de datos
O.J.P	Información, Seguridad Nacional	Dato	Información estatal	Dato, Información
Pena C.P	6 a 9 años	2 meses a 2 años	3 a 6 años	1 a 5 años
Pena COIP	1 a 3 años y 5 a 7 años	3 a 5 años	1 a 3 años	5 a 7 años

DELITO	Daño Informático	Destrucción de instalaciones para transmisión de datos	Apropiación ilícita	Estafa
ARTÍCULO C.P.	Art.415.1	Art.415.2	Art.553.1	Art.563 inc.2
ARTÍCULO COIP	Art.232	Art.232	Art.190	Art.186, 190
S.A	Cracker	Delincuente Informático	Delincuente Informático	Delincuente Informático
S.P	Agraviado, perjudicado: El Estado y Sector Público	Agraviado, perjudicado	Agraviado, perjudicado	Agraviado, perjudicado
V.R	Destruir, alterar, inutilizar, suprimir, dañar programas y bases de datos	Destrucción, alteración, inutilización de infraestructura física	Apropiación de lo ajeno	Cometa delitos utilizando medios electrónicos
O.J.P	Dato, Seguridad Nacional	Propiedad	Propiedad	Propiedad, Intimidad
Pena C.P	6 meses a 3 años y 3 a 5 años	8 meses a 4 años	6 meses a 5 años	6 meses a 5 años
Pena COIP	3 a 5 años	3 a 5 años	1 a 3 años	1 a 3 años y 5 a 7 años