Alexander Cuenca Espinosa

EL DELITO INFORMÁTICO EN EL ECUADOR "UNA NUEVA TENDENCIA CRIMINAL DEL SIGLO XXI" SU EVOLUCIÓN, PUNIBILIDAD Y PROCESO PENAL

Quito – Ecuador

2012

Alexander Cuenca Espinosa[1]

I. Preliminar

De los casos suscitados en Ecuador 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 GMS y Kaspersky, los delitos informáticos en Ecuador 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 solo 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 de este tipo de delitos.[3]

II. Planteamiento del problema

El problema de los llamados Delitos Informáticos se suscita con la aparición de la tecnología y con las nuevas formas de delinquir, es así que, con la evolución de la tecnología, a la par ha habido una línea cronológica de continuos nuevos "modus operandi" en la era digital que han culminado con una variedad de delitos, en este caso informáticos.

---

[1] Estudiante de último año de la Pontificia Universidad Católica del Ecuador. Mediador Certificado por la Pontificia Universidad Católica del Ecuador. Investigador en Informática Forense por RED-LIF. Certified Ethical Hacker por EC-Council USA. CEO y Fundador LEXTECH CORPORATION Ecuador. Cyber Crime Researcher. Miembro de la Red Iberoamericana de Derecho Informático. Miembro de la Red Latinoamericana de Informática Forense. Miembro de CriptoRed de la Universidad Politécnica de Madrid. Representante por Ecuador del proyecto mundial "Net Against Cyberfraud" propuesto por la Universidad de Castilla-La Mancha en España. Co-fundador de la Comunidad "Free Security Ecuador". Miembro de la Comisión Académica de la Asociación Escuela de Derecho 2011. Miembro de Directorio de la Asociación Escuela de Derecho 2012. Ex Investigador Forense y Judicial del Departamento Nacional de Investigaciones de la Fiscalía General del Estado de Ecuador. Coordinador del 1er Taller de Litigación Oral Penal avalado por el Colegio de Abogados de EE-UU (American Bar Association). Organizador de varios eventos académicos.
Cursos Especializados: Curso de Diplomado "International Law and Protection Rights", University for Peace, San José - Costa Rica (Candidato); Curso de Derecho Penal en la Especialización "Delitos Informáticos", Instituto de Altos Estudios Universitarios / Universidad de Granada-España; Course of International Finance, Stanford University, USA; Course of Computer Science, Harvard University, USA. Ponente en varias conferencias en cuanto a Seguridad Informática, Derecho Informático y Cibercrimen. Ponente invitado para las conferencias sobre Derecho y Nuevas Tecnologías (Marzo/2013) en la Universidad de Salamanca-España. Autor de escritos académicos e investigaciones en cuanto a Delitos Informáticos a nivel nacional e internacional. Autor de libro: El Delito Informático en el Ecuador. Contacto.- E-mail: manager@lextechcorp.com / Twitter: Abg_AlexanderCE

[2] ABOGADOS EC, http://www.abogados.ec/2011/02/estadisticas-2010-delitos-informaticos-en-ecuador/

[3] DIARIO LA HORA, http://www.lahora.com.ec/index.php/noticias/show/1101278706#.UKl6DYZMfTo

Uno de los grandes problemas que surgen en torno a los Delitos Informáticos es saber si el legislador tiene el conocimiento adecuado para tipificar éstos y si existen las herramientas y/o actualizaciones necesarias para que los jueces puedan juzgar este tipo de ilícitos, siendo la respuesta NO. Vemos que en caso de tipificar y juzgar este tipo de ilícitos quedan en la total ineficacia, ya que no contamos con profesionales a fines a estos temas que puedan, de manera proba y garantizada, hacer punible y efectiva la justicia en estos actos antijurídicos.

III. Definición de Delito Informático

Aunque no hay una definición específica acerca de "Delito Informático", varios tratadistas y doctrinarios en el tema han hecho el esfuerzo por dilucidar un concepto claro y conciso respecto a este ilícito de la nueva era. Es así que entre los más conocidos tenemos las siguientes definiciones:

Nidia Callegari define al *"delito Informático" como "aquel que se da con la ayuda de la informática o de técnicas anexas".* El **Departamento de Investigación de la Universidad de México**, señala como delitos informáticos *"todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático".* El italiano **Carlos Sarzana**, define el Delito Informático como *"cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo".* **María de la Luz Lima** dice que el *"delito electrónico" "en un sentido amplio es cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el Delito Informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin".*[4]

Después de revisar varias definiciones de algunos autores, he seleccionado la provista por el Profesor chileno **Renato Jijena Leiva**, quien 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".*[5]

A definición personal *"el delito informático es toda actividad en la cual se utilizan medios computacionales, telemáticos o electrónicos para el cometimiento de un delito; delitos que constituyen nuevas formas penales que incluyen como elementos primogénitos al internet como instrumento abstracto y a la computadora como instrumento físico"*[6]. El delito informático en sus diferentes tipos es un delito susceptible de ser sancionado por el código penal, siempre y cuando la figura antijurídica se encuentre configurada en el tipo y establecida en un cuerpo normativo. El delito informático dependiendo su resultado deberá tener un alto índice de reprochabilidad para la no reincidencia del mismo.[7]

---

[4] CONDE O'DONNELL, Hugo; http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf; Argentina; 2009

[5] LEIVA JIJENA, Renato; "CHILE, LA PROTECCIÓN PENAL DE LA INTIMIDAD Y EL DELITO INFORMÁTICO", Editorial Andrés Bello; CHILE 1992, p. 225

[6] El autor

[7] Ídem

IV. Evolución del Delito Informático en Ecuador y el mundo

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 como elementos primogénitos al internet (como instrumento abstracto) y a la computadora (como instrumento físico).

Cabe señalar que desde el año 2009 en el Ecuador ya se puso en discusión el tema de imponer penas a los delitos informáticos. Estas penas que se impondrían fueron ya discutidas en el proyecto para la creación de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, ley que un principio tuvo sus falencia por el desconocimiento de la materia, es decir, por el desconocimiento por parte de profesionales en cuanto a delitos informáticos, ya que como es obvio era una tendencia criminal que 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 en el año 2002, en la promulgación de la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos[9], fueron artículos posteriormente incluidos en el Código Penal. El boom que consiguió que de forma apresurada se concluyera con el proyecto de dicha ley para su posterior publicación, fue por uno de los primeros ataques a website en el país, a través de la técnica del Defacing[10], el ataque a la página del Municipio de Quito en el año 2001[11]. Vale recordar también que el primer delito informático que se cometió en el Ecuador fue en el año 1996, en un caso conocido, que fue denunciado pero que nunca obtuvo sentencia: el redondeo de cantidades que se efectuaba en las planillas realizadas por el antiguo EMETEL, caso en el cual se desconocía a donde se dirigían estas cantidades (que muchas veces eran demasiado pequeñas para que cause discusión), pero que juntadas, formaban un monto de dinero muy apreciable. Para este tipo de delito informático se utilizó la técnica del Salami o Rounding Down.[12]

---

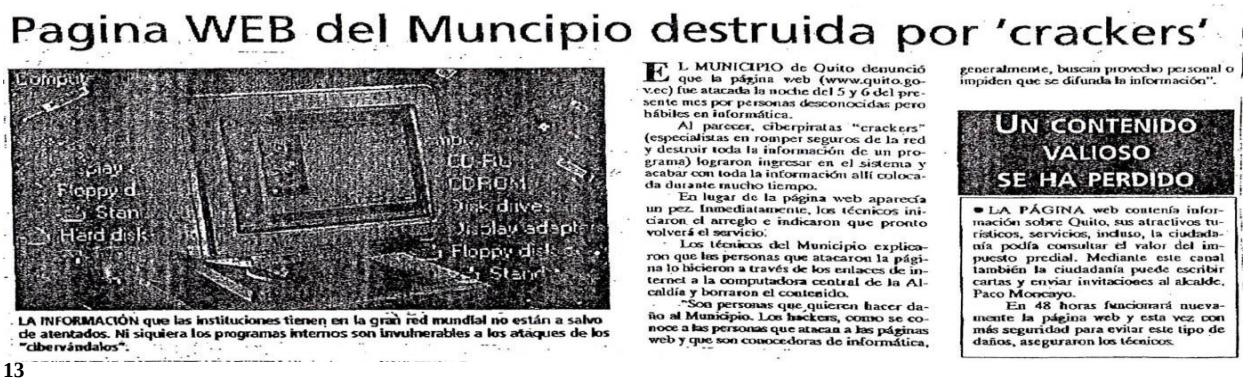
[8] DELITOS INFORMÁTICOS INFO, http://delitosinformaticos.info/delitos_informaticos/definicion.html

[9] Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, R.O. Suplemento 557 de 17-ABR-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] Fuente: Diario Hoy, año 2001 "Hackean página del Municipio de Quito"

[12] 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)



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.

13

En cuanto a la evolución del delito informático en el caso concreto ecuatoriano, encontramos estos nuevos delitos realizados a través de medios y plataformas electrónicas:

- Delitos Bancarios en el E-Banking (estafa bancaria y el desvío de dinero)
- Acoso Escolar electrónico o cyber bullying (maltrato psicológico y verbal mediante plataformas electrónicas)
- Grooming o Acoso Sexual (a menores por internet)
- Chantaje informático (a una persona adulta o infante que parte del bullying y grooming)
- Sabotaje informático (dañar medios informáticos con un fin determinado)
- Terrorismo informático (medios electrónicos por pulsaciones para activar instrumentos electromagnéticos)
- 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 como chats)
- Pornografía intantil (para intercambio de material pornográfico de menores de edad, en Ecuador el caso más conocido es Gigatribe)
- Espionaje informático (filtración de información pública como Wikileaks)
- Infiltración electrónica
- Piratería Informática (Legalización de esta a través del SRI, caso tiendas de material cinematográfico pirata)
- Usurpación de claves (Keylogging, Phishing a través de spam, scams e ingeniería social)
- Violación de correo electrónico
- Robo de Identidad (alto costo en el mercado negro, lo más común información de Hotmail y Facebook, oscila entre 300 a 600USD)
- Seguridad en Sistemas biométricos (huellas dactilares o contra respuestas al sistema biométrico instalado)
- Falsificación de documentos electrónicos
- Falsificación de firma electrónica (certificados electrónicos provenientes de estas)
- Planeación o simulación de delitos convencionales
- Apropiación indebida (rooteo de servidores es un tipo de hurto)
- Clonación de tarjetas de crédito (a través de skimmers)
- Delitos tributarios (falsificación electrónica de asientos contables)

[13] DIARIO HOY, Archivo Histórico; Página web del Municipio de Quito destruida por "crackers"; 6-XII-2001; N.I.

V. Delitos Informáticos tipificados en la legislación ecuatoriana

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos más conocida como Ley 67, publicada en el R.O. / Sup.557 del 17 de Abril del 2002 tuvo un avance muy importante en el sentido de incluir figuras penales que hagan punibles los ilícitos informáticos con lo cual, junto al Código Penal, integran normas creadas para la Sociedad de la Información.

Dentro de estas normas promulgadas en la Ley 67 posteriormente incluidas al Código Penal, constan los siguientes ilícitos informáticos:

- Art.57 LCEFEMD: **Infracciones informáticas.-** Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

- Art.58 LCEFEMD, Conc. Art.202.1 CP: **Contra la Información Protegida.-** El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva, o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

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

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

- Art.58 últ.inc LCEFEMD, Conc. Art.202.2 CP: **Obtención y utilización no autorizada de información.-** La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica.

- Art.59 LCEFEMD, Conc. Art.262 CP: **Destrucción Maliciosa de Documentos.-** Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier

mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo.

- Art.60 LCEFEMD, Conc. Art.353.1 CP: **Falsificación electrónica.-** Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

  1.- Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial;
  2.- Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad;
  3.- Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.
  El delito de falsificación electrónica será sancionado de acuerdo a lo dispuesto en este Capítulo.

- Art.61 LCEFEMD, Conc. Art.415.1 CP: **Daños informáticos.-** El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica.

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

- Art.61 últ.inc LCEFEMD, Conc. Art.415.1 CP: **Destrucción de instalaciones para transmisión de datos.-** Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.

- Art.62 LCEFEMD, Conc. Art.553.1 CP**: Apropiación ilícita.-** Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o

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

- Art.62 últ.inc LCEFEMD, Conc. Art.553.2 CP**: Pena.-** La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:
  1. Inutilización de sistemas de alarma o guarda;
  2. Descubrimiento o descifrado de claves secretas o encriptadas;
  3. Utilización de tarjetas magnéticas o perforadas;
  4. Utilización de controles o instrumentos de apertura a distancia; y,
  5. Violación de seguridades electrónicas, informáticas u otras semejantes.

- Art.63 LCEFEMD, Conc. Art.563 inc.2 CP**: Estafa. -** Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.

- Art.64 LCEFEMD, Conc. Art.606.20 CP**: Violación Derecho a la Intimidad.-** Los que violaren el derecho a la intimidad, en los términos establecidos en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

VI. Delitos informáticos y comentarios dentro del borrador del Código Orgánico Integral de Garantías Penales

En la nueva reforma del Código Penal actual prevista para diciembre del 2012, tenemos nuevos ilícitos entre los cuales figuran los informáticos, estos ilícitos han sido tipificados y adecuados al tipo, ya que, recientemente ha ido aumentado la diversificación de estos delitos así como sus modus operandi, dejando a la víctima en un estado de indefensión por no encontrarse un delito establecido en la ley, y más allá por no facilitar los mecanismos para la pronta reparación del agravio. Si bien una persona se encuentra perjudicada lo que busca es justicia, pero una justicia expedita, mas no tardía. Es así que a continuación citaré algunos de los artículos en materia penal que se integran a la reforma ya citada para hacer punible un ilícito de este tipo.

Tipos penales que se adecúan al delito informático:

- **Artículo 85.- Trata de personas.-** Comete trata de personas quien participe antes, durante o después de una o más de las siguientes acciones: captar, custodiar, trasladar, acoger, recibir, entregar personas con fines de explotación, recurriendo a la amenaza, violencia, engaño o ***cualquier forma de fraude***.[14]

- **Artículo 91.- Comercio de órganos.-** La persona que sin cumplir con los requisitos legales, realice actos de simulación jurídica que tenga por objeto la intermediación

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

onerosa, o ***negocie por cualquier medio***[15], obtenga, posea, almacene, traslade órganos, tejidos, fluidos, células, componentes anatómicos o sustancias corporales será sancionada con pena privativa de libertad de catorce a dieciséis años.

- Si las actividades referidas en el inciso anterior se realizan con órganos, tejidos, fluidos, células, sustancias corporales o cualquier material anatómico que provenga de personas vivas, la pena privativa de libertad será de dieciséis a diecinueve años.
- Si la infracción se ha cometido en personas de grupos de atención prioritaria, se sancionará con pena privativa de la libertad de diecinueve a veinticinco años.
- Si la persona que realiza la infracción es un profesional de la salud, a más de las penas señaladas en este artículo quedará inhabilitado en forma permanente para el ejercicio de su profesión o actividad.

- **Artículo 96.- Pornografía con utilización de niñas, niños o adolescentes.-** La persona que utilice, niñas, niños o adolescentes para fotografiar, filmar, grabar, producir, divulgar, ofrecer, vender, comprar, poseer, portar, almacenar, trasmitir[16] o exhibir, ***por cualquier medio***[17], para uso personal o intercambio, representaciones reales o simuladas de su imagen o voz en actividad sexual o eróticas, reales o simuladas, explícitas e implícitas o la representación de sus genitales con fines sexuales será sancionada con pena privativa de libertad de once a catorce años.

  - La misma pena se aplicará a quien, en las condiciones indicadas en el inciso anterior, promueva, financie, fabrique, reproduzca, publique, importe, exporte, difunda, o distribuya material pornográfico para fines de explotación sexual, ***por cualquier medio sea directo, mecánico, digital, audio visual, o con soporte informático, electrónico o de otro tipo.***
  - Si la víctima además de las circunstancias descritas en el primer inciso, sufre de algún tipo de discapacidad o una enfermedad grave o incurable, se sancionará con pena privativa de libertad de dieciséis a veinticinco años.
  - Cuando la o el infractor sea el padre, madre, parientes hasta el cuarto grado de consanguinidad o segundo de afinidad, tutores, representantes legales, curadores, personas del entorno íntimo de la familia, ministros de culto, profesores, maestros o personas que por su profesión o actividad haya abusado de la víctima, será sancionado con pena privativa de libertad de dieciséis a veinticinco años.

- **Artículo 148.- Tortura.- La persona que por cualquier medio**, inflija intencionadamente a otra persona, grave dolor o sufrimiento, ya sea de naturaleza física o psíquica; o lo someta a condiciones o métodos que anulen su personalidad o disminuyan su capacidad física o mental, aun cuando no causen dolor o sufrimiento físico o psíquico;

[15] 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.
[16] La transmisión, divulgación y envío de estos se comete a diario, entre los casos conocidos en Ecuador tenemos a GIGATRIBE, en donde una red de pedófilos mantenía en internet alojados más de 200GB de pornografía infantil.
[17] Revisar documental "Pederastas en la Red" – Canal Cuatro, España

con cualquier finalidad en ambos supuestos, será sancionada con pena privativa de libertad de cinco a siete años.
La persona que incurra en alguna de las siguientes circunstancias será sancionada con pena privativa de libertad de siete a nueve años:

- Aproveche cualquier ***grado de conocimiento técnico***[18] para aumentar el dolor de la víctima.
- Se cometa por parte de una persona que es funcionaria o servidora pública, o por un particular que actúe bajo sus órdenes, o con la aquiescencia de aquel.
- Se cometa en persona con discapacidad, menor de dieciocho años, mayor de sesenta y cinco años o mujer embarazada.
- La o el servidor público que tenga competencia para evitar la comisión de la infracción de tortura y omita hacerlo será sancionado con pena privativa de libertad de tres a cinco años.

- **Artículo 159.- Atentados sexuales a menores de dieciocho años a través de medios electrónicos.-** La persona que a través de ***medio electrónico o telemático*** seduzca o intente seducir con fines de connotación sexual a una persona menor de dieciocho años de edad o proponga concertar un encuentro con la misma a fin de cometer cualquiera de las infracciones previstas en este capítulo, siempre que tal propuesta se acompañe de actos materiales encaminados al acercamiento, será sancionada con pena privativa de libertad de tres a cinco años, sin perjuicio de las penas correspondientes a las infracciones en su caso cometidas. Se impondrá el máximo de la pena cuando el acercamiento se obtenga mediante coacción o intimidación.

  La persona que utilice o facilite el correo tradicional, medios electrónicos o telemáticos o cualquier otro medio de comunicación para ofrecer servicios sexuales con menores de dieciocho años de edad será sancionada con pena privativa de libertad de cinco a siete años.

- **Artículo 166.- Incitación al odio.-** La persona que públicamente por ***cualquier medio incite al odio***, al desprecio, o a cualquier forma de violencia moral o física contra una o más personas en razón del color de su piel, sexo, religión, origen nacional o étnico,

[18] Si se lo comete a través de plataformas electrónicas se suscita el Cyberbullying más conocido como "Ciberacoso", el mismo que según R.B.Stalken consiste en causar angustia emocional, preocupación, y tiene como propósito legítimo la comunicación por vías electrónicas. El **Ciberacoso** puede ser tan simple como continuar mandando e-mails a alguien que ha dicho que no quiere permanecer en contacto con el remitente. El **Ciberacoso** puede también incluir amenazas, connotaciones sexuales, etiquetas peyorativas (p.ej., discurso del odio).
Se ha comentado muchas veces que del Cyberbullying deriva a un "Grooming" o "Acoso Sexual Electrónico" que a su vez recae en el resultado del llamado "Chantaje Electrónico", propiamente por un fin pecuniario.

orientación sexual o identidad sexual, edad, estado civil o discapacidad, será sancionada con pena privativa de libertad de seis meses a dos año.[19]

- **Artículo 169.- Violación de la intimidad.-** Será sancionada con pena privativa de libertad de seis meses a dos años, la persona que realice alguna de las siguientes conductas:
    - Capte o grabe sin consentimiento palabras de otra no emitidas públicamente, mediante cualquier tipo de instrumentos, ***procesos técnicos u otros medios.***[20]
    - Capte o grabe sin consentimiento imágenes de otra persona, mediante cualquier tipo de ***instrumentos, procesos técnicos u otros medios***.[21]
    - Capte o grabe las ***comunicaciones telemáticas*** de otra sin su consentimiento.
    - Acceda a la información contenida en ***soportes informáticos*** de otra, sin su consentimiento.[22]
    - Si las conductas descritas en los números anteriores se cometen por una persona en ejercicio de un servicio o función pública, será sancionada con pena privativa de libertad de uno a tres años.
    - La divulgación de las palabras, imágenes, conversaciones, ***telecomunicaciones***, informaciones o grabaciones que no sean de conocimiento público, obtenidas mediante cualquiera de las conductas descritas en los números anteriores, será sancionada con pena privativa de libertad de uno a tres años. [23]
    - No son aplicables estas normas para la persona que divulgue grabaciones de audio y video en las que interviene única y personalmente.

- **Artículo 170.- Violación de comunicación privada.-** La persona que acceda, intervenga o retenga sin autorización judicial o de su titular, ***cualquier tipo de comunicación privada*** no destinada a ella, será sancionada con pena privativa de libertad seis meses a dos años.
  La divulgación del contenido de la comunicación privada, obtenida mediante cualquiera de las conductas descritas en el inciso anterior, será sancionada con pena privativa de libertad de uno a tres años.

---

[19] Dentro del contexto de "Odio", en el acontecer diario 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.

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

[21] Keylogger (revisar para más información)

[22] Robo de información en cuentas de e-mail y bancarias.

[23] En la mayoría de casos esta información de carácter 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 información llamada PASTEBIN (www.pastebin.com).

La servidora o servidor militar o policial que, sin la debida autorización legal, intercepte, examine, retenga, grabe o difunda correspondencia o comunicaciones privadas o reservadas de cualquier tipo y ***por cualquier medio***, será sancionada con pena privativa de libertad de seis meses a dos años.

- **Artículo 175.- Difamación.-** La divulgación, ***por cualquier medio de comunicación social*** u otro de carácter público, excepto la autorizada por la ley, de los nombres y apellidos de los deudores ya sea para requerirles el pago o ya empleando cualquier forma que indique que la persona nombrada tiene aquella calidad, será sancionada con pena privativa de libertad de seis meses a dos años.

- **Artículo 180.- Extorsión virtual.**- La persona que tenga información suficiente de otra, de su actividad profesional, laboral, social o familiar, que extorsione a los miembros de su familia o personas allegadas, para obtener un beneficio personal o económico, mediante engaños de un supuesto plagio, será sancionada con pena privativa de libertad de cinco a siete años.

- **Artículo 180.- Estafa.-** La persona que para obtener un beneficio patrimonial antijurídico, para sí mismo o para un tercero, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, para que realice un acto patrimonial que perjudique su patrimonio o el de un tercero, será sancionada con pena privativa de libertad de dos a cinco años. Igual pena tendrá la persona que:

    1. *Defraude mediante* ***el uso de tarjeta de crédito, débito o compra, cuando ella hubiere sido alterada, clonada, duplicada,*** *hurtada, robada u obtenida sin legítimo consentimiento de su propietario.*
    2. Entregue en calidad de administradora o administrador, apoderada o apoderado, corredora o corredor de una bolsa de valores, o agente de valores, certificación falsa sobre las operaciones o inversiones que se realicen en ella.
    3. Induzca a la compra o venta pública de valores por medio de cualquier acto, práctica, mecanismo o artificio engañoso o fraudulento.
    4. Efectúe cotizaciones o transacciones ficticias respecto de cualquier valor, sea que las transacciones se lleven a cabo en el mercado de valores o a través de negociaciones privadas.
    5. La persona que perjudique a más de dos personas, o si el monto del perjuicio es igual o mayor a cincuenta salarios básicos unificados del trabajador en general será sancionada con pena privativa de libertad de cinco a siete años.
    6. La estafa cometida a través de una institución del Sistema Financiero Nacional o se utilicen fondos públicos o de la Seguridad Social será sancionada con pena privativa de libertad de siete a nueve años.

- **Artículo 184.- Aprovechamiento ilícito de servicios públicos.-** La persona que, de manera ilícita, ***mediante cualquier mecanismo clandestino o alterando los sistemas de control*** o aparatos contadores, se aproveche de los servicios públicos de energía eléctrica[24], agua, derivados de hidrocarburos, gas natural, gas licuado de petróleo o señal de telecomunicaciones y otros para provecho personal o de terceros, será sancionada con pena privativa de libertad de uno a tres años.

  Igual pena recibirá la servidora o servidor público que permita o facilite la comisión de la infracción u omita efectuar la denuncia de la comisión de la infracción.

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

- **Artículo 186.- Apropiación fraudulenta por medios electrónicos.-** La persona que ***utilice fraudulentamente un sistema informático o redes electrónicas*** y de telecomunicaciones, para facilitar la apropiación de un bien ajeno, o la persona que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sanciona-da con pena privativa de libertad de tres a cinco años.

  La misma sanción se impondrá si la infracción se hubiese cometido con inutilización de sistemas de alarma o guarda; descubrimiento o descifra-do 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.

  La persona que altere los números de serie físicos y electrónicos que identifican un equipo terminal de telefonía móvil, o esté en tenencia de infraestructura para el efecto; que active y comercialice estos equipos robados o hurtados; será reprimida con la misma penas. Sin perjuicio de las sanciones administrativas y adopción de medidas cautelares conforme a la Ley Especial de Telecomunicaciones.

- **Artículo 206.- Violación de derechos conexos de autor.-** La persona que en violación de los derechos de autor o derechos conexos:

  - Reproduzca un número mayor de ejemplares de una obra que el autorizado por el titular.

[24] Existe el caso de un hacker chileno llamado ux0r0b0r quien penetró el sitio de la Empresa Eléctrica Quito, ingresando al sistema en donde se controla toda la conexión eléctrica de Quito desde el internet. Pueden ver el vídeo del ataque en: www.segu-info.org

- Introduzca al país, almacene, ofrezca en venta, venda, arriende o de cualquier otra manera ponga en circulación o a disposición de terceros reproducciones de obras en número que exceda del número autorizado por el titular.
- Retransmita por cualquier medio la emisiones de los organismos de radiodifusión.
- Introduzca al país, almacene, ofrezca en venta, venda, arriende o de cualquier otra manera ponga en circulación o a disposición de terceros aparatos u otros medios destinados a descifrar o decodificar las señales codificadas o de cualquier otra manera burlar o quebrantar los medios técnicos de protección aplicados por el titular del derecho.
- Será sancionada con pena privativa de libertad de uno a tres años y multa de tres a treinta salarios básicos unificados del trabajador en general.
- Incurre en este delito, también, la persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas o en general información contenida o soportada en las tarjetas de crédito, débito, pago o similares.[25]

- **Artículo 208.- Supresión, alteración o suposición de la identidad y estado civil.-** La persona que impida, altere, añada o suprima la inscripción de los datos de identidad en ***programas informáticos***, partidas, tarjetas índices, cédulas y cualquier otro documento emitido por la Dirección General de Registro Civil, Identificación y de Cedulación o sus dependencias, de sí o de otra persona; inscriba en la Dirección General de Registro Civil, Identificación y de Cedulación a una persona que no es su hijo como propio o que no existe; o que mediante la utilización de fuerza física o psicológica o viciando el consentimiento, obligue a otra a contraer matrimonio consigo o con tercera persona, será sancionada con pena privativa de libertad de uno a tres años.

  La persona que altere la identidad de una niña o niño; la sustituyere por otra; suponga un embarazo o parto; entregue o consigne datos falsos o supuestos sobre un nacimiento; usurpare la legítima paternidad o maternidad de una niña o niño; o, declarare falsamente el fallecimiento de un recién nacido, será sancionada con pena privativa de libertad de uno a tres años.

- **Artículo 209.- Suplantación de identidad.-** La persona que de ***cualquier forma*** suplante la identidad a otra persona, será sancionada con pena privativa de libertad de seis meses a dos años.

- **Artículo 228.- Revelación ilegal de base de datos.-** La persona que revele información registrada en un banco de datos cuyo secreto esté obligado a preservar por disposición de una ley, será sancionada con pena privativa de libertad de uno a tres años.

[25] Se adecúa a la figura de delito informático llamada CARDING, que consiste en la falsificación y duplicación de las bandas de las tarjetas de crédito y débito. En el Ecuador el número de casos por estos delitos sobrepasa los 500.

Si esta conducta se comete por parte de una persona en ejercicio de un servicio o función pública, empleados bancarios internos o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.

- **Artículo 229.- Daño informático.-** La persona que acceda, interfiera, interrumpa, modifique, altere, suprima, intercepte o desvíe ilícitamente sistemas informáticos o telemáticos, imagen, dato, mensaje o emisiones electromagnéticas proveniente de un sistema informático que los transporte, será sancionada con pena privativa de libertad de tres a cinco años.

- **Artículo 230.- Obtención de información.-** La persona que copie, clone, modifique, desarrolle, trafique, comercialice, ejecute, programe o imite una página electrónica, enlaces o ventanas emergentes, con la finalidad de obtener la información ahí registrada o disponible, será sanciona-da con pena privativa de libertad de siete a nueve años.

  En la misma sanción incurrirá la persona que modifique el sistema de re-solución de nombres de dominio, de tal manera que haga entrar al usuario a una dirección o sitio de internet diferente a la que quiere acceder, ya sea a su banco o a otro sitio personal o de confianza.

- **Artículo 231.- Modificación de programas.-** La persona que altere, manipule o modifique el funcionamiento de un programa o sistema informático o telemático, o un mensaje de datos para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de ésta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años y multa de veinte a treinta salarios básicos unificados del trabajador en general.

  Con igual pena serán sancionadas cuando obtengan mediante engaños, información, datos o claves personales o secretas para acceder a sistemas informáticos o telemáticos.

- **Artículo 232.- Inutilización de programas.-** La persona que, destruya, impida u obstaculice el funcionamiento o el acceso normal, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, redes, enlaces de comunicaciones, información o cualquier mensaje de datos contenidos en un sistema de información o telemático, red electrónica o sus componentes lógicos, será sancionada con pena privativa de libertad de tres a cinco años.

  Con igual pena serán sancionadas las personas que:
  - Produzcan, trafiquen, adquieran, envíen, introduzcan, vendan o distribuyan de cualquier manera, software malicioso o programas destinados a causar los efectos señalados en el primer inciso de este artículo; o,
  - Destruyan o alteren sin la autorización de su titular, la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de información en general.

- La pena será de cinco a siete años de privación de la libertad si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la defensa nacional.

- **Artículo 233.- Infracciones contra la información pública clasificada legalmente.-** La servidora o servidor militar o policial que, utilizando cualquier medio electrónico, informático o afín, obtenga información clasificada de conformidad con la ley, será sancionada con pena privativa de libertad de tres a cinco años.

    - A la persona que destruyere o inutilizare este tipo de información, se le aplicará la misma pena privativa de libertad.
    - La divulgación o la utilización de la información así obtenida, será sancionada con pena privativa de libertad de cinco a siete, siempre que no se configure otra infracción de mayor gravedad.
    - Si la divulgación o la utilización fraudulenta son realizadas por parte de la persona o personas encargadas de la custodia o utilización legítima de la información, éstas serán sancionadas con pena privativa de libertad de siete a nueve años.

- **Artículo 305.- Defraudación tributaria.-** Constituye defraudación todo acto de simulación, ocultación, omisión, falsedad o engaño que induzca a error en la determinación de la obligación tributaria o por los que se deja de pagar en todo o en parte los tributos realmente debidos, en provecho propio o de un tercero; así como aquellas conductas que contravienen o dificulten las labores de control, determinación y sanción que ejerce la administración tributaria.

  Son casos de defraudación los siguientes:

    - 9. Alterar dolosamente, 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.
    - 10. Llevar doble contabilidad, deliberadamente, con distintos asientos en libros o registros informáticos, para el mismo negocio o actividad económica.

- **Artículo 306.- Defraudación aduanera.-** 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 privativa de libertad de tres a cinco años y multa de tres a diez veces el valor de los tributos que se pretendió evadir, si realiza cualesquiera de los siguientes actos:

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

- **Artículo 331.- Captación ilegal de dinero.-** La persona que organice, desarrolle y promocione ***por cualquier medio***, de forma pública o clandestina, actividades de

intermediación financiera sin autorización legal, destinadas a captar ilegalmente dinero del público en forma habitual y masiva, será sancionada con pena privativa de libertad de cinco a siete años y multa de cien a doscientos salarios básicos unificados del trabajador en general.

Las mismas penas se aplicarán a la persona que realice operaciones cambiarias o monetarias sin autorización de la autoridad competente.

Serán comisados los instrumentos utilizados en la comisión de la infracción, así como los productos o réditos obtenidos.

- **Artículo 335.- Falsificación y uso de documento falso.-** [26]La persona que falsifique, destruya o realice cualquier alteración que varíe los efectos o sentido de los documentos públicos o sellos nacionales, establecidos por la ley para la debida constancia de ciertos hechos y actos de relevancia jurídica, será sancionada con pena privativa de libertad de tres a cinco años. El uso de estos documentos falsos será sancionado con pena privativa de libertad de uno a tres años.

- **Artículo 361.- Destrucción de registros.-** La persona que destruyan de cualquier modo, registros auténticos o instrumentos originales de autoridad pública o procesos judiciales, será sancionada pena privativa de libertad de seis meses a dos años.

- **Artículo 367.- Apología de la infracción.-** La persona que por **cualquier medio** haga apología de la infracción, o de una persona sentenciada por un delito, por razón del acto realizado será sancionado con multa de tres salarios básicos unificados del trabajador en general.

- **Artículo 369.- Espionaje[27].-** La servidora o servidor militar que en tiempo de paz realice uno de estos actos, será sancionada con pena privativa de libertad de siete a nueve años:

  1. Obtenga, difunda, falsee o inutilice información clasificada legalmente y que su uso o empleo por país extranjero o atentare 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;

  3. Envíe documentos, informes, gráficos u objetos que ponga en riesgo la seguridad o la soberanía del Estado, sin estar obligado a hacerlo; o, de estar obligado por la fuerza, no pusiere tal hecho en conocimiento de las autoridades inmediatamente;

[26] Pueden considerarse documentos materiales y electrónicos.
[27] Revisar caso de espionaje militar del agente de inteligencia "Bradley Manning" quien entregó información confidencial de EE-UU a Wikileaks

5. Altere, suprima, destruya, desvíe, incluso temporalmente, información u objetos de naturaleza militar relevantes para la seguridad, la soberanía o la integridad territorial.

- **Artículo 377.- Terrorismo.-** Será sancionado con pena privativa de libertad de once a quince años, el que individualmente o formando asociaciones, armados o no, pretextando cualquier fin, inclusive políticos, provoque o mantenga, en estado de terror a la población o a un sector de ella, mediante actos que pongan en peligro la vida, la integridad física o la libertad de las personas o a las edificaciones o medios de comunicación, transporte, valiéndose de medios capaces de causar estragos; en especial:

  La persona que, colocando un artefacto o sustancia, o por cualquier medio[28], destruya, dañe o perturbe el funcionamiento de una edificación pública o privada, plataforma fija marina, así como de las instalaciones o servicios de transportación terrestre, navegación aérea o marítima, si tales actos, por su naturaleza, constituyen un peligro para la seguridad de la transportación terrestre, de las aeronaves o naves, como de la seguridad de las plataformas y demás edificaciones.

- **Artículo 378.- Financiación del terrorismo.-** Las personas que dolosamente, en forma individual o colectiva, de manera directa o indirecta, ***por cualquier medio***[29], proporcionen, ofrezcan, organicen o recolecten fondos o activos, de origen lícito o ilícito, con la intención de que se utilicen o a sabiendas de que serán utilizados para financiar en todo o en parte, la comisión de las infracciones de terrorismo; o cualquier otro acto destinado a causar la muerte o lesiones corporales graves a un civil o a cualquier otra persona que no participe directamente en las hostilidades en una situación de conflicto armado, cuando, el propósito de dicho acto, por su naturaleza o contexto, sea intimidar a una población u obligar a un gobierno o a una organización internacional a realizar un acto o a abstenerse de hacerlo; o, la existencia de terroristas individuales, grupos u organizaciones terroristas; serán sancionados con pena privativa de libertad de seis a nueve años.

VII. Casos más importantes y conocidos en Ecuador

- **Emetel 1996 (Técnica del Salami)**
  Este caso trata sobre el redondeo de cantidades que se efectuaba en las planillas realizadas por el antiguo EMETEL, caso en el cual se desconocía a donde se dirigían estas cantidades (que muchas veces eran demasiado pequeñas para que cause discusión), pero que juntadas, formaban un monto de dinero muy apreciable. Para este tipo de delito informático se utilizó la técnica del **Salami o Rounding Down.**
  Este caso que aunque conocido, en su tiempo jamás obtuvo una sentencia para los responsables.

[28] Revisar caso de bombas que se activan a través de pulsaciones electromagnéticas empleando un computador, laptop o celular a distancia. Casos más comunes realizados en Irak.
[29] Hoy por hoy organizaciones terroristas organizan y recolectan dinero por internet para la financiación de armas y demás con propósito de terrorismo.

- **Phishing Banco del Pichincha (2009-2012)**
  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 entraba a un sitio bancario y seguro, donde posteriormente ingresaba su información como: username, passwords y claves e-keys, las cuales después facilitarían al ciberdelincuente a cometer el delito. Entre los bancos más afectados se encontraron el Banco del Pichincha, Banco de Guayaquil, Banco Amazonas, Banco Proamérica, entre otros.

- **Carding a bancos ecuatorianos(2010-2011)**
  Banco Amazonas (Av. Amazonas y Villalengua) ATM65
  Dentro de los casos de delitos informáticos a tarjetas de crédito, está el perpetrado en un cajero automático: 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 almacenaba información de decenas de usuarios para la posterior duplicación de estas tarjetas de crédito, las cuales serían utilizadas con fines comerciales, como compras por internet y con fines lucrativos, como el retiro de dinero de otros cajeros.

  Hasta diciembre del año 2011, se presentaron 140 denuncias de tarjetas clonadas a través de este cajero. De las investigaciones realizadas se descubrió que los autores eran parte de una banda de crimen organizado, compuesta por ciudadanos colombianos y peruanos.

- **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 de protesta al 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 la independencia de los medios de comunicación en contra de un gobierno autoritarista.

- **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.[30]

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.[31]

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, donde la policía, en su investigación, dio a conocer que la direcciones IP's de donde se habían subido dichas imágenes provenían de Ecuador. Indicado este hecho y siendo éste un delito transnacional, la organización que se hizo cargo del caso fue la Interpol. Es por ello que los documentos investigados en Australia fueron remitidos a la Interpol de Melbourne (en dicho país), para su posterior envío a la Interpol de Lyon en Francia, luego a la de Londres en Reino Unido, a la de Buenos Aires en Argentina y finalmente a la Interpol de Quito en Ecuador. Una vez que los documentos se encontraron en Ecuador, la Fiscalía General del Estado junto a Interpol, DGI y Policía Judicial prosiguieron con las investigaciones que dieron como resultado final la localización de los autores del ilícito, quienes se encontraban en la ciudad de Guayaquil.

- **Cable filtrados**
  - **Wikileaks Embajada USA (2011)**

En el 2011, la organización mundial Wikileaks, comandada 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 e indicaciones del 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, pidiendo de forma inmediata el abandono del país de la embajadora estadounidense, Heather Hodges, a quien la declararon como persona no grata en Ecuador.

- **Grupos de Hacking (2012)**

Ataques diarios a websites

Diariamente se cometen ataques a websites no solo ecuatorianas, sino a nivel mundial. Algunos de estos ataques son perpetrados por ecuatorianos, personas aficionadas a la tecnología e informática, las cuales penetran en diversos sitios con el propósito de dejar su *marca personal*, es decir, un signo o huella que dé a entender que ellos estuvieron ahí.

[30] «GigaTribe brings private P2P sharing to U.S.». *CNET News* (17 de noviembre de 2008).
[31] BRENNER, Susan; «Gigatribe and the 4th Amendment» ; (25 de junio de 2010).

Ciertamente, en Ecuador hay personas con el talento suficiente para emplear este conocimiento en beneficio del país, más no lo hacen. Esto porque, según ellos y según entrevistas realizadas, no hay el incentivo tanto pecuniario como laboral para que dichas personas puedan dedicarse a estas labores, con el fin de proteger al sistema informático gubernamental ecuatoriano. En el país normalmente para el ataque a páginas web utilizan la técnica del "Defacing", antes ya mencionada en este artículo.

De los grupos conocidos en Ecuador de hacking podemos destacar a: Ecuadorian Hacking Team, Kalimndor Team, Fenix Hackers, Anon Azules, Anon Ecuador, Latin Hack Team y otras menos conocidas, pero que igualmente perpetran ataques a diario.

VIII. Legislación base en materia de Derecho Informático en contra de ilícitos informáticos

- Constitución
- Código Penal
- Código civil
- Código de Procedimiento Penal
- 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 comercio electrónico, firmas electrónicas y mensaje de datos
- Ley de protección de usuarios del sistema financiero
- Ley de derechos de autor
- Ley especial de telecomunicaciones
- Ley Orgánica de Transparencia y Acceso a la Información Pública
- Proyecto de Ley Orgánica de Comunicación

IX. Proceso Penal del Delito Informático en el Ecuador

- LA INSTRUCCIÓN FISCAL Y LA POLICÍA JUDICIAL
    - Policía Judicial
        - Investigación, cadena de custodia
    - La indagación previa y la instrucción fiscal
        - Fijarse si hay autores, coautores, cómplices o encubridores
        - Si no hay indicios de delito el Fiscal ordena el archivo provisional o definitivo del expediente (indagación hasta dos años)
        - Si hay indicios de delito se apertura la instrucción fiscal (información necesaria y suficiente para deducir imputación)
        - Partes procesales, declaración del procesado, intervención del ofendido y del imputado.
        - Duración máximo 90 días.

En Ecuador, en cuanto a Delitos Informáticos, se realiza la denuncia a través del Ministerio Público, es decir, a través de la Fiscalía General del Estado, quien cuenta con la cooperación internacional de la Interpol (por el problema de una o más jurisdicciones), y de manera local con el Servicio de Inteligencia de la Policía Judicial y Contrainteligencia, para las debidas capturas y seguimientos.

Esta cooperación internacional con la Interpol es regulada por el **Red de Contactos 24/7**[32] para el TRATAMIENTO DE DATOS. Además la Fiscalía ha hecho convenios en los cuales el responsable del caso puede solicitar a empresas internacionales como Facebook, Yahoo o Hotmail su cooperación para la investigación de estos ilícitos.

- ETAPA INTERMEDIA
  - La audiencia preliminar
    - Sustanciación del ilícito
    - Los sujetos anunciarán pruebas que serán presentadas en el juicio

- ETAPA DE JUICIO
  - Presentación de pruebas y formulaciones
  - Sustanciación antes el Tribunal de Garantías Penales
    - Comprobar culpabilidad o inocencia
  - Sentencia
    - Condenatoria o absolutoria

- ETAPA DE IMPUGNACIÓN
  - Diferentes recursos a presentar
  - El recurso depende de la instancia

X. Eficacia probatoria del documento electrónico

El Art.2 Ley de Comercio Electrónico, firmas electrónicas y mensaje de datos señala: ***"Los mensajes de datos tendrán igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta ley y su reglamento***".

En concordancia con la legislación chilena en el Art.1 inc2. Ley de Firma Electrónica chilena nos dice ***"la ley se inspira en el principio de la equivalencia del soporte electrónico al soporte de papel"***[33]

Es así que dentro de esta teoría de la equivalencia de la prueba documental tiene igual compensación siendo mensaje de dato o papel escrito.

[32] Interpol ha creado el sistema mundial de comunicación policial I-24/7 a fin de conectar entre sí a los funcionarios encargados de la aplicación de la ley de todos los países miembros, lo que permite a los usuarios autorizados intercambiar información policial vital y acceder a las bases de datos y a los servicios de INTERPOL 24 horas al día.

[33] Art.1 inciso 2 Ley de Firma Electrónica Chilena

XI. Punibilidad de un Delito Informático

Para ser punible un acto, se necesita de elementos probatorios o llamados también en investigación forense *elementos de convicción*. Los elementos de convicción son el conjunto de pruebas (electrónicas) necesarias para la comprobación de un delito, sin las cuales fuese imposible imponer una pena a este ilícito. Estas pruebas deben ser mostradas como fidedignas por medio de un informe pericial. Para que esta pericia o experticia sea válida debe ser realizada por peritos avalados por el Concejo de la Judicatura o peritos privados, según lo señala la normativa para la acreditación de peritos, en sus artículos 11 y 12 publicada en el año 2009.

Cabe destacar que dentro del derecho informático existe la refutación de la prueba cuando no se muestre con seguridad y certeza su credibilidad, es así que en caso de ser ilegítima, esta es nula e inválida en el proceso.

XII. A manera de conclusión

Dentro del paradigma que envuelve a los delitos informáticos en el Ecuador, hay una gran problemática que requiere la toma de medidas para solventar y solucionar estos delitos, ya que, en un principio, los delitos informáticos quedan impunes, debido a que no se encuentran en una normativa propiamente dicha. Es decir que, pese a que en el Código Penal ecuatoriano hay pocas figuras que hacen punibles estos delitos, no todas se adecuan al tipo, dejando en la total indefensión al agraviado, ya que al no considerarse como delitos en el Código Penal, no se les puede establecer una pena o si bien se las establece puede ser asemejando otro ilícito, aquí la falencia no sería sólo de quien juzga, sino también del órgano administrador de justicia, pues en Ecuador no hay cursos o seminarios de actualización constantes sobre estos delitos a jueces, fiscales y demás funcionarios públicos.

A criterio personal, en primer lugar, en el Ecuador se debería crear un cultura tecnológica, en la cual, a las anteriores y nuevas generaciones de ciudadanos, se les guíe y eduque sobre los mecanismos de protección para no ser víctimas de delitos informáticos; en segundo lugar se debería dar prioridad a estos delitos, tipificándolos de una forma adecuada y ordenada, ya que al cometerse estos, en su mayoría, afectan la parte económica de una persona; y cómo último punto, se debería dar prioridad al empleo de personas con la capacidad intelectual para lo que se llama "seguridad informática", ya que estas personas serían las encargadas de proteger todo el sistema integral y tecnológico del Estado ecuatoriano.

****

Bibliografía

LEIVA JIJENA, Renato; "CHILE, LA PROTECCIÓN PENAL DE LA INTIMIDAD Y EL DELITO INFORMÁTICO", Editorial Andrés Bello; CHILE 1992

PÁEZ, Juan José y ACURIO DEL PINO, Santiago; Derecho y Nuevas Tecnología, Editora Corporación de Estudios y Publicaciones, Año 2010

MÁRQUEZ ESCOBAR, Carlos; El Delito Informático, Editorial Leyer; Colombia 2003

LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS, R.O. Suplemento 557 de 17-ABR-2002, Quito-Ecuador

DIARIO HOY, Archivo Histórico; Página web del Municipio de Quito destruida por "crackers"; 6-XII-2001

MENSAJE DE DATOS; Comisión de las Naciones Unidas para el Derecho Mercantil Internacional (CNUDMI); 2000.

LEY DE FIRMA ELECTRÓNICA CHILENA, 2003.

CÓDIGO PENAL ECUATORIANO; Editora Corporación de Estudios y Publicaciones; Marzo 2009

CÓDIGO CIVIL ECUATORIANO; Editora Corporación de Estudios y Publicaciones; 2010

CÓDIGO PROCEDIMIENTO CIVIL ECUATORIANO; Editora Corporación de Estudios y Publicaciones; 2011

SEGUNDO BORRADOR PROYECTO DE LEY PARA CÓDIGO ORGÁNICO INTEGRAL PENAL; Asamblea Constituyente, 2011

ARAUJO GRANDA, M.Paulina; APUNTES DE CLASE SOBRE DELITOS EN PARTICULAR, 2012.

Netgrafía

CONDE O'DONNELL, Hugo;
http://dmi.uib.es/~dmiamp/TEGP/Tema%202/Delito%20informatico%20I%20pres.pdf; Argentina; 2009

DELITOS INFORMÁTICOS INFO; http://delitosinformaticos.info/delitos_informaticos/definicion.html

GIGATRIBE; «GigaTribe brings private P2P sharing to U.S.». *CNET News* (17 de noviembre de 2008).

BRENNER, Susan; «Gigatribe and the 4th Amendment» ; (25 de junio de 2010).

ABOGADOS EC;
http://www.abogados.ec/2011/02/estadisticas-2010-delitos-informaticos-en-ecuador/

DIARIO LA HORA;
http://www.lahora.com.ec/index.php/noticias/show/1101278706#.UKl6DYZMfTo

NOTA: El artículo original tuvo una extensión de más de 30 páginas, por recomendación de los editorialistas se eliminaron y modificaron muchas de ellas.