FACULTAD DE DERECHO Y CIENCIAS SOCIALES

RETOS DE LA ADMINISTRACIÓN DE JUSTICIA PENAL FRENTE A LOS DELITOS INFORMÁTICOS EN EL ECUADOR

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar por el título de Abogado de los Tribunales y Juzgados de la República

Profesor Guía

Dra. Elsa Jacqueline Guerrero Carrera

Autora

Katherine Alexandra Hernández Maldonado

Año

2016

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

_____

Dra.Elsa Jacqueline Guerrero Carrera

Magister en Derecho

C.I.: 2000027470

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mí autoría, que se han citado las fuentes correspondientes y que en su ejecución, se respetaron las disposiciones legales que protegen los derechos de autor vigentes”

_____

Katherine Alexandra Hernández Maldonado

C.I.: 172258050-1

DEDICATORIA

Este trabajo de titulación y mi esfuerzo, está dedicado a mis padres, Alexandra Maldonado y Hugo Parra, también a mis abuelos, quienes siempre supieron brindarme el apoyo para culminar con mi carrera.

AGRADECIMIENTOS

Agradezco a mis padres que siempre supieron guiarme y apoyarme para cumplir mis anhelos, les agradezco por haber estado a mi lado todo este tiempo; a la vez agradezco a la Universidad por haberme dado la oportunidad de prepararme y a la doctora Jacqueline Guerrero quien supo guiarme para realizar este trabajo.

RESUMEN

El presente ensayo trata sobre los delitos informáticos y la complejidad que existe para su investigación y sanción, como premisas para el análisis de la realidad de la administración de justicia penal del Ecuador en este tema.

El Ecuador tiene tipificadas varias conductas, que se enmarcan en el concepto de delitos informáticos, esto es aquellas conductas que emplean cualquier tipo de tecnología en el cometimiento de un ilícito. Pero considerando que la investigación de los mismos no es similar a la de un delito común, la administración de justicia afronta importantes retos para lograr una efectiva criminalización secundaria.

Los principales obstáculos que actualmente tienen las instituciones encargadas de investigar y sancionar los delitos conocidos como delitos informáticos, son: la falta de capacitación del personal; la ausencia de convenios internacionales que permitan la investigación transnacional; la disposición de herramientas tecnológicas necesarias para la investigación de los delitos que se cometen en el ciberespacio; la existencia de infraestructura tecnológica limitada, entre otras.

ABSTRACT

The present essay is about the cybercrime and its complexity that exists for the investigation and punishment, as premises for the analysis of the true reality of the administration of criminal justice in Ecuador on this issue.

Ecuador has classified several behaviors that are part of the concept of cybercrime, behaviors that uses technology to commit a crime.

But considering that the investigation of these crimes is not similar to the common crime, the administration of justice faces important challenges for an efficient secondary criminalization.

The main obstacles that institutions responsible for the investigations and punishment of these crimes known as cybercrimes are: lack of trained staff; the absence of international agreements that allow transnational research; the provision of technological tools necessary for the investigation of crimes committed in the cyberspace; the existence of limited technological infrastructure, among others.

ÍNDICE

INTRODUCCIÓN 1

1. GENERALIDADES DE LOS DELITOS INFORMÁTICOS 2

1.1. Consideraciones previas 2

1.2 Conceptualización 4

1.3 Clasificación doctrinaria 6

1.4 Complejidad de los delitos informáticos 8

2. LA ADMINISTRACIÓN DE JUSTICIA PENAL DEL ECUADOR FRENTE A LOS DELITOS INFORMÁTICOS 13

2.1. Los delitos informáticos en el Ecuador 13

2.1.1. Tipificación 13

2.1.2. La investigación de los delitos informáticos 19

2.1.3. Proceso investigativo y actores 22

2.2. Realidad procesal 25

2.3 Retos y desafíos 31

REFERENCIAS 35

ANEXOS 37

INTRODUCCIÓN

El presente trabajo pretende evidenciar los retos y desafíos que debe afrontar la administración de justicia penal del Ecuador en relación con los delitos informáticos, debido a su naturaleza y complejidad.

Con tal objetivo se realizó un análisis exegético y dogmático de la norma legal vigente, esto es el Código Orgánico Integral Penal, puesto que era necesario identificar los distintos delitos informáticos y sus respectivas sanciones. También se apeló a la lectura de textos especializados, a fin de tener una mejor comprensión de los aspectos técnicos de los delitos informáticos y finalmente se realizó un estudio empírico para conocer, de fuente directa, el tratamiento que se da a los delitos informáticos por parte de las distintas instituciones que están llamadas a atenderlos. Por tal razón se empleó la técnica de la entrevista a personal de las instituciones que están ligadas al tratamiento de los ciberdelitos; y se recopiló información de fuentes primarias.

El ensayo fue estructurado en dos partes; la primera destinada a describir generalidades de los delitos informáticos, su conceptualización y clasificación; y, en la segunda parte se explica el tratamiento que se da a los delitos informáticos en la legislación ecuatoriana, con especial énfasis en la realidad procesal, esto es el proceso de investigación que se realiza en las diferentes unidades e instituciones que colaboran con la Fiscalía.

En la parte final del ensayo constan las conclusiones del trabajo, siendo la principal que el Ecuador cuenta con la tipificación y las sanciones para diferentes conductas que se conocen como delitos informáticos, pero tiene muchos retos y desafíos en cuanto a la criminalización secundaria, pues los delitos informáticos tienen un alto grado de complejidad para ser investigados, por lo que se requiere de un personal debidamente capacitado, con amplios conocimientos, no solamente en el ámbito del derecho sino con preparación especializada en informática; a la vez es necesario contar con herramientas tecnológicas que permitan realizar una investigación eficaz, entre otras.

1. GENERALIDADES DE LOS DELITOS INFORMÁTICOS

1.1. Consideraciones previas

En el siglo XXI es irrefutable el impacto que han tenido las tecnologías de la información y comunicación en prácticamente todas las actividades del quehacer humano; día a día la tecnología avanza y se transforma vertiginosamente, brindándonos nuevas formas de relacionarnos, trabajar y enfrentar al mundo. Uno de los mayores beneficios de los avances tecnológicos son las formas de comunicación y el acceso a la información sobre diversos temas, sin mayores límites; esta facilidad nos ofrece el internet y los avanzados sistemas de comunicación.

A esto se suman los sistemas informáticos que las empresas utilizan para su gestión y atención a los clientes; todo este conjunto de nuevas formas de hacer las cosas han dando paso a la globalización, permitiendo agilizar la forma de hacer negocios, de transmitir mensajes y recibir información.

A pesar de todas las ventajas que nos han traído estas tecnologías, el acceso indiscriminado a la información tiene aspectos negativos; por ejemplo, no todas las publicaciones que se encuentran en el ciberespacio provienen de personas calificadas, no todos los contenidos que se encuentran es las redes son verídicos y/o probados científicamente; además, los avances tecnológicos han permitido que surjan nuevas formas de delinquir.

Si miramos hacia atrás, internet desde su inicio ha sido usado para cometer actos ilícitos, pretendiendo generar ataques a las empresas que lo empleaban; las primeras en sufrir abusos fueron las empresas telefónicas, estos actos son anteriores al siglo XX, y se descubrieron cuando varias personas fueron sorprendidas abusando de redes telefónicas en los EE.UU (Smartekh, s.f.).

A finales de 1990 las empresas quedaron expuestas a riesgos significativos debido a la delincuencia informática; fueron perjudicadas en su patrimonio financiero y/o intelectual (Smartekh, s.f.).

Las personas que hacen uso de la tecnología para cometer ilícitos son conocidos como cibercriminales o ciberdelincuentes y han estado presentes desde que se empezó a usar el internet para el comercio (Smartekh, s.f.). Este uso negativo de la tecnología ha puesto en jaque a diversas industrias, llegando incluso a comprometer a los gobiernos de varios países, por lo que las naciones han sentido la necesidad de reconocer a estos actos como delitos informáticos.

En las últimas décadas el porcentaje de delitos informáticos ha aumentado dramáticamente y han ido tornándose de un inconveniente menor a un riesgo significativo, hay casos de intrusión en los sistemas, que no pasaron de esto, pero hay otros casos en los que se han implantado rutinas informáticas para hacer transferencias económicas o robo de fórmulas y conocimientos que constituyen el capital intelectual de las empresas.

Todas estas acciones han obligado a que las empresas tanto privadas como estatales gestionen sistemas de seguridad para el acceso a sus plataformas informáticas y con mayor empeño si estos tienen salida a las redes públicas que conforman el internet.

Dando crédito a estos actos tecnológicos delictivos las naciones se han unido y han creado convenios, que permiten facilitar la investigación de estas acciones; el primero con este fin es el Convenio de Budapest, que fue aprobado en el año 2001, y se enfoca en la ciberdelincuencia. El Ministerio del Interior de España (s.f.) afirma que es uno de los primeros tratados que se orienta en delitos informáticos y delitos en internet.

> “Es un documento que constituye un hito en la lucha coordinada y eficaz contra este tipo de conductas y que en la actualidad ha sido suscrito por muchos de los Estados integrados en el Consejo de Europa y del que también son signatarios algunos otros países no pertenecientes a ese marco como, EEUU, Japón, Canadá y Sudáfrica” (CN-CERT *Cent*ro Criptológico Nacional, s.f.).

Las Naciones Unidas también han creado una unidad que se ocupa de los delitos informáticos, con el objetivo de aportar al reconocimiento y clasificación de delitos informáticos (Naciones Unidas, s.f.).

Con lo expuesto se demuestra la seriedad con que el mundo está reaccionando ante los delitos informáticos, por lo que se organiza, norma y sanciona estas conductas.

1.2 Conceptualización

Muchos tratadistas consideran que es difícil definir los delitos informáticos, en razón de que estos no existen en forma específica, es decir no se trata de una conducta que puede ser catalogada como tal, sino que se trata de un conjunto de conductas. Afirman que simplemente existen delitos que se realizan o se comenten utilizando medios informáticos.

Miguel Ángel Davara (2008) sostiene que el delito informático es la “acción que reuniendo las características que delimitan el concepto de delito, es llevada a cabo utilizando un elemento informático y/o telemático, o vulnerado los derechos del titular de un elemento informático, ya sea hardware o software” (pp. 358-359).

La definición de la (UNODC) Oficina de las Naciones Unidas contra la Droga y el Delito (2005), señala que los delitos informáticos son una:

> “Conducta proscrita por la legislación y/o la jurisprudencia, que implica la utilización de tecnologías digitales en la comisión del delito; se dirige a las propias tecnologías de la computación y las comunicaciones; o incluye la utilización incidental de computadoras en la comisión de otros delitos” (Naciones Unidas, s.f.).

Para Julio Téllez (s.f.) existen dos definiciones dependiendo el caso, el primer concepto que menciona es el atípico, el cual establece que los delitos informáticos son: “Actitudes ilícitas en que tienen a las computadoras como

instrumento o fin"; otra de las definiciones que Téllez sostiene es un concepto típico, que señala: "Las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin" (p. 82).

Por su parte Santiago Acurio (2007), uno de los expertos en este tema de Ecuador, menciona que, la delincuencia informática es:

> "Todo acto o conducta ilícita e 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" (p. 14).

Es necesario mencionar que la doctrina, da distintas denominaciones a las conductas que se realizan a través de la tecnología, como delitos informáticos, delincuencia informática o ciberdelincuencia.

Existen varias definiciones respecto a estos delitos, y no hay un concepto en el que todos los autores coincidan exactamente, la razón posiblemente sea por las distintas formas en las que se usa la tecnología para cometer ilícitos; a esto hay que añadirle la dificultad de saber con efectividad y en tiempo real los avances tecnológicos.

Por esto se entendería que se trata de enmarcar a estos ilícitos en conceptos amplios, que se tornen flexibles y abarquen la mayoría de acciones que se puedan cometer ilícitamente, a través del uso de la tecnología informática y de comunicaciones.

Analizando los conceptos citados, también podemos indicar que la amplitud de estos se debe a las nuevas formas de delinquir, que se van desencadenando por el conocimiento tecnológico que los actores adquieren en esta materia.

Creemos que por estas razones los expertos no formulan conceptos específicos de delito informático, ya que en un futuro cercano podríamos tener legislaciones inconclusas.

Además nos damos cuenta que estos delitos, están vinculados a otros preexistentes en las normas penales; pero por el medio por el que se realizan se convierten en delitos informáticos, lo que dificulta su clasificación, definición e inclusión en los cuerpos jurídicos de los Estados.

En el libro Derecho Penal Informáticos de Santiago Acurio (2015), le cita al Parker que considera que un delito informático es: “todo acto intencional asociado de una manera u otra a los computadores; en los cuales la víctima ha o habría podido sufrir una pérdida; y cuyo autor ha o habría podido obtener un beneficio” (p. 44).

Por ende, entendemos que el delito informático se lo puede conceptualizar como un acto ilegal que busca el beneficio del actor y que se concretiza con la utilización de cualquier dispositivo tecnológico, ya que en la actualidad existen dispositivos avanzados que pueden irrumpir en las redes de comunicación, sistemas informáticos y transmiten/receptan cualquier dato, facilitándose la ejecución de actos ilícitos, estos dispositivos por su portabilidad inclusive ayudan al anonimato del actor.

1.3 Clasificación doctrinaria

El Convenio de Budapest es una guía para las legislaciones de cada Estado, a la vez que llama a los países a tomar en cuenta algunas pautas a seguir, para que la investigación que se hace frente a estos delitos sea eficaz. A través de este convenio se buscó facilitar la detección, investigación y la respectiva sanción, tanto nacional como internacional, por lo que menciona algunos tipos de delitos informáticos, que los Estados deben observar al momento de tipificar conductas.

En el Convenio de Budapest se sistematizan nueve conductas, en cuatro grupos que se clasifican de la siguiente forma:

- Infracciones contra la confidencialidad y disponibilidad de datos y sistemas.

- Infracciones relativas al contenido.
- Infracciones contra la propiedad intelectual y derechos afines.
- Infracciones informáticas.

A pesar que este es uno de los primeros convenios que se preocupó de la criminalidad informática, y da algunos parámetros para que los países puedan hacer una correcta tipificación, no todos los Estados son parte de este convenio, incluso el Ecuador.

Para dar una clasificación de los delitos informáticos se debe tomar en cuenta dos cosas, el medio o el fin; por un lado el medio es el instrumento que se usa para cometer el delito; mientras que el fin es el beneficio que obtendrá el sujeto que realice el ilícito (Davara, 2008, p. 363).

Según Miguel Ángel Davara (2008), existen seis clasificaciones frente a estos delitos que se detallan a continuación:

- Manipulación en los datos e información, contenidos en los archivos o soportes físicos informáticos ajenos.
- Acceso a los datos y utilización de los mismos por quien no está autorizado para ello.
- Introducción de programas o rutinas en otros ordenadores para destruir información datos o programas.
- Utilización del ordenador y/o los programas de otra persona, sin autorización, con el fin de obtener beneficios propios y en perjuicio de otro.
- Utilización del ordenador con fines fraudulentos.
- Agresión a la privacidad mediante la utilización y procesamiento informático de datos personales con fin distinto al autorizado (pp. 363 – 367).

Daniel Altmark y Eduardo Molina (2012), mencionan que las clasificaciones de este tipo de delitos debe realizarse considerando el bien jurídico que se quiere

proteger y dentro de cada categoría se debe distinguir las conductas típicas de la vida cotidiana; consideran que esto es la base para tener una tipificación en esta materia, en la que se contemplen las necesidades que en realidad se requieren en la legislación (p.239). Proponen la siguiente clasificación:

- Delitos contra el patrimonio
- Delitos contra la intimidad
- Delitos contra la seguridad pública y las comunicaciones
- Falsificaciones informáticas
- Contenidos ilegales en internet

1.4 Complejidad de los delitos informáticos

Muchos autores que analizan la complejidad para tipificar, sancionar e inclusive investigar los delitos informáticos, indican que estos actos no solamente evolucionan con la sociedad como es el caso de los delitos que ya han sido tipificados específicamente en los cuerpos jurídicos, sino que también evolucionan conforme al avance tecnológico.

El Centro Criptológico Nacional en su artículo que se titula “El 95% de los ciberdelitos cometidos quedan impunes” menciona que:

> “La rapidez, el anonimato, la comodidad y la facilidad de las nuevas tecnologías hacen que los delincuentes las aprovechen para sus actividades, tanto para las "tradicionales" como para otras más novedosas, como ataques a sistemas informáticos, robo, manipulación de datos, usurpación de identidad, actividades de pederastia, estafas comerciales y bancarias mediante diferentes métodos que ya han sido reconocidos como el pishing, la difusión de virus o troyanos, etc.” (CCN-CERT Centro Criptológico Nacional, s.f.).

Así como también menciona que “el alcance mundial de estas actividades criminales ha causado alarma en todos los gobiernos del mundo, que han puesto en marcha medidas legislativas para prevenir y castigar tales conductas” (CCN-CERT Centro Criptológico Nacional, s.f.).

De acuerdo a lo anotado previamente vemos que, además de los convenios internacionales, se han creado organismos privados que dan seguimiento a los ciberdelitos y creemos que esto está ligado al esfuerzo que están realizando las organizaciones para gestionar y encontrar formas de prevención e investigación, que vayan de la mano con las formas de cometer delitos a través de la tecnología.

Como menciona Erwin Chiluiza (2015), “el medio electrónico se ha convertido en un blanco para cometer diferentes actos ilegales tales como: extorsión, robo, fraude, suplantación de identidad, entre otros. La delincuencia informática es difícil de comprender o conceptualizar plenamente, a menudo se la considera una conducta relegada por la legislación, que implica la utilización de tecnologías para la comisión del delito“ (Chiluiza, 2015, párr. 2).

En el Ecuador no se contempla claramente un verdadero proceso investigativo para los delitos informáticos, Edwin Pérez experto, en la página de la fiscalía, menciona que en nuestro país existen dificultades durante la investigación de ilícitos respaldados por el uso de la tecnología, por cuanto la información cruzada a nivel de redes sociales o cuentas de correos electrónicos no se encuentran almacenados en el país, en razón de que los grandes proveedores de redes sociales y los generadores de los sistemas informáticos de uso masivo tienen sus bancos de datos en otros países, principalmente en Estados Unidos (Fiscalía General del Estado, s.f.).

Es necesario mencionar que un gran problema que tiene el país frente a estos delitos es que Ecuador no es parte de los convenios internacionales, lo que indiscutiblemente merma la capacidad de realizar investigaciones con el alcance que se requiere, porque no podemos recurrir a los otros Estados para realizar cruces de información, tomando en cuenta que la mayor parte de estos delitos se realizan usando internet, lo que provoca que se utilicen medios que

están fuera del país y al no disponer de la trazabilidad de estos actos ilícitos se alargan los procesos investigativos.

Por otro lado Edwin Pérez, considera que la investigación de los ciberdelitos es compleja, debido al desconocimiento de técnicas en la investigación y la falta de coordinación interinstitucional del sector a cargo de las telecomunicaciones (Fiscalía General del Estado, s.f.).

Revisando estas publicaciones entendemos que el país tiene una gran desventaja frente a la investigación de estos delitos, ya que el personal especializado de las distintas instituciones, que se encargan en estas investigaciones, tienen una capacitación básica y no tienen los suficientes conocimientos de las distintas formas o técnicas que existen para tener una investigación eficiente.

Necesariamente se debería dar una exhaustiva capacitación referente a la criminalidad informática, tanto teórica como práctica; es importante que esta formación no solo se les imparta a los investigadores o peritos, sino también a jueces y magistrados.

Creemos que esto es importante, porque estos pueden tener una confusión al momento de impartir justicia, ya que estos delitos tienden a ser confundidos con los delitos tradicionales; muchos de estos delitos son simplemente acoplados porque se usan herramientas tecnológicas al ser cometidos (Verne, s.f. p.87).

La Fiscalía ha estado consciente de las falencias que tiene al momento de enfrentar este tipo de investigaciones, por esta razón busca que sus funcionarios se capaciten por lo que por ejemplo, el 2015 se desarrolló un taller para la investigación de los Ciberdelitos, donde expertos brasileños impartieron sus charlas, con el objetivo de que el personal se interese por esos temas y se especialice en procedimiento técnico para la investigación, cadena de custodia de la evidencia digital (Fiscalía General del Estado, s.f.).

Se menciona que otro de los objetivos de esta charla fue ayudar a reforzar el conocimiento de programas informáticos y su aplicación; determinando las

circunstancias en que se cometió el delito, autores y cómo obtener pruebas materiales, ya sea dentro o fuera del país (Fiscalía General del Estado, s.f.).

Edwin Pérez, quien es mencionado en la página web de la Fiscalía, agrega que “la única forma de lograr un combate eficaz es la adquisición de tecnología para investigar los ciberdelitos, que solo puede conseguirse a través de la suscripción de convenios internacionales con la grandes multinacionales” (Fiscalía General del Estado, s.f.).

Se requiere la participación de varios países para combatir estos delitos, porque muchas veces los actores intervinientes no se encuentran en el mismo país en el que está la persona afectada, este es un grave problema que existe; se requiere mayor rigurosidad para determinar los actores ya que se está abusando del uso de las tecnologías para causar daños a terceros.

Por otro lado debemos considerar a los sujetos que intervienen en los delitos informáticos, es otra arista de esta temática que agrega complejidad a la investigación y sanción de estos, ya que puede ser fácil determinar la persona o institución afectada, muchas veces a través de las denuncias realizadas. El problema más grande radica en detectar quién es la persona que atacó un sistema, vulneró seguridades, realizó fraudes utilizando los datos robados o que está haciendo uso indebido de la tecnología, pero para determinar con precisión los sujetos y actos realizados se necesita de herramientas tecnológicas especializadas para realizar auditorías forenses y de expertos en el tema para la investigación.

En los delitos informáticos existen dos tipos de sujetos involucrados, los sujetos activos y a los sujetos pasivos:

Para José Rebolo (2009, p.9), el sujeto activo es quien comete el delito; tratándose de delitos informáticos estas personas por lo general poseen habilidades especiales, en razón de que estas personas manejan sistemas informáticos, son expertos en la informática, pero no necesariamente tienen formación en el área; pues cada vez hay más jóvenes que cometen delitos informáticos.

Las aptitudes o la capacidad que tiene una persona en el ámbito informático no es un indicador de delincuencia informática, mientras que otros autores mencionan que si lo es, en razón de los delincuentes informáticos que son personas capaces y listas para realizar cosas que un sujeto cualquiera no lograría hacer (Acurio, 2015, p.56).

Además está el sujeto pasivo, quien es la persona que sufrió la afectación, es decir la víctima. Como indica Santiago Acurio (2015, p.82), este sujeto es la persona titular del bien jurídico que el legislador protege y sobre la cual recae la actividad del sujeto activo.

En los delitos informáticos los actores se denominan de igual forma que en cualquier tipo penal; por ejemplo, en el caso de un robo el delincuente será denominado sujeto activo y la persona perjudicada se denominará sujeto pasivo; esta es una de las razones por las que se puede afirmar que los delitos informáticos son delitos que se están acoplando al derecho penal.

2. LA ADMINISTRACIÓN DE JUSTICIA PENAL DEL ECUADOR FRENTE A LOS DELITOS INFORMÁTICOS

2.1. Los delitos informáticos en el Ecuador

En 1999 el Ecuador se interesó en los delitos informáticos porque se iniciaron las discusiones del proyecto de Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Esta norma jurídica entró en vigencia en abril de 2012 e introdujo una reforma al Código Penal vigente a la época, por lo que desde esa fecha el país contó con las primeras tipificaciones de las conductas conocidas como delitos informáticos.

Desde el 2014 el Ecuador cuenta con el Código Orgánico Integral Penal, que unificó la materia penal. Esta norma mantuvo la tipificación de los denominados delitos informáticos, que estaban propuestas en el Código Penal anterior, como consecuencia de las reformas que introdujo la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, también eliminó conductas e incorporo nuevas.

Un estudio realizado por el observatorio de la ciberseguridad en América Latina y el Caribe, detalla que la población ecuatoriana es de 15.902.916, y que el número de personas que tienen acceso a internet, es de 6.838.254, es decir el 43% de la población (Observatorio de Ciberseguridad, s.f. p.70). Si este porcentaje tiene acceso al internet; herramienta mediante la cual se comete la mayoría de ilícitos cibernéticos, no sabemos qué porcentaje tiene el verdadero conocimiento de los ciberataques que pueden estar sufriendo.

A continuación se sintetiza todas las conductas previstas en el COIP, que encajan en el concepto de los denominados delitos informáticos.

2.1.1. Tipificación

Considerando que, el COIP no establece un título referente a los delitos informáticos utilizaremos una tabla que tiene por finalidad proporcionar mayor

coherencia acerca de la dimensión y análisis de estos delitos, y, para tal fin, agrupamos los delitos practicados por medios de dispositivos electrónicos en cuatro grupos:

1. Delitos contra la integridad sexual y reproductiva
2. Delitos contra el derecho a la intimidad personal y familiar
3. Delitos contra el derecho a la propiedad
4. Delitos contra la seguridad de los activos de los sistemas de información y comunicación,

Tabla 1. Tipificación de delitos en el COIP

Delitos contra la integridad sexual y reproductiva			
	Artículo	**Delito**	**Sanción**
	Art. 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	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. 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.	Pena privativa de libertad de 1 a 3 años. Pena privativa de libertad de 3 a 5 años.
	Art. 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	La persona, que utilice o facilite el correo electrónico, chat, mensajería instantánea, redes sociales, blogs, fotoblogs, juegos en red o cualquier otro medio electrónico o telemático para ofrecer servicios sexuales con menores de dieciocho años de edad,	Pena privativa de libertad de 7 a 10 años
Delitos contra el derecho a la intimidad personal y familiar			
	Art. 178.- Violación a la intimidad.	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,	Pena privativa de libertad

		información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio. No son aplicables estas normas para la persona que divulgue 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.	de 1 a 3 años.
	Art. 229.- Revelación ilegal de base de datos	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. 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 realicen intermediación financiera o contratistas.	Pena privativa de libertad de1 a 3 años Pena privativa de libertad de 3 a 5 años.
Delitos contra el derecho a la propiedad			
	Art. 190.- 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 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. 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.	Pena privativa de libertad de 1 a 3 años
	Art. 191.- Reprogramación o modificación de información de equipos terminales móviles	La persona que reprograme o modifique la información de identificación de los equipos terminales móviles.	Pena privativa de libertad de 1 a 3 años.

	Art. 195.- Infraestructura ilícita	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. No constituye delito, la apertura de bandas para operación de los equipos terminales móviles.	Pena privativa de libertad de 1 a 3 años
	Delitos contra la seguridad de los activos de los sistemas de información y comunicación		
	Art. 230.- Interceptación ilegal de datos.-	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.	Pena privativa de libertad de 3 a 5 años
	Art. 231.- Transferencia electrónica de activo patrimonial.	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. 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.	Pena privativa de libertad de 3 a 5 años.
	Art. 232.- Ataque a la integridad de sistemas	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	Pena privativa de libertad

	informáticos	de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen. 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.	de 3 a 5 años. Pena será de 5 a 7 años de privación de libertad.
	Art. 233.- Delitos contra la información pública reservada legalmente.	La persona que destruya o inutilice información clasificada de conformidad con la Ley. La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información. 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.	Pena privativa de libertad de 5 a 7 años. Pena privativa de libertad de 3 a 5 años. Pena privativa de libertad de 7 a 10 años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se

			configure otra infracción de mayor gravedad
	Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones	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.	Pena privativa de la libertad de 3 a 5 años.

Adaptado de (Código Orgánico Integral Penal, 2014)

Analizando los diferentes delitos tipificados en el COIP se puede establecer que los bienes jurídicos protegidos son los mismos que se tutelan en un delito común; se les atribuye una pena privativa de libertad, si es que son cometidos con el uso de herramientas tecnológicas, y como podemos darnos cuenta, sus sanciones no son apegadas a la forma de ejecución, ya que como se evidencia en varios artículos simplemente se enfocan en dar un castigo por el resultado del acto.

La inclusión de penas ha aportado positivamente para que las personas que han sufrido alguna afectación de sus derechos o que fueron víctimas de actos dolosos, a través de cualquier medio tecnológico, sientan que ya existen leyes que los amparan; es así que muchas personas que han sido víctimas de estos delitos, accedan a la justicia. Conforme lo estableció la Fiscalía, en la actualidad se registran más denuncias que cuando no estaba en vigencia el COIP; se evidencia que desde el 10 de agosto de 2014 hasta el 31 de mayo de 2015 se registran 626 denuncias por este tipo de delitos. (Fiscalía General del Estado, s.f.).

Se esperaría que con estas denuncias y la necesidad que están generando, tanto en investigación como sanción, se vaya buscando una forma más

específica para tipificar a estos delitos, porque involucran más situaciones ilegales que un delito común; por ejemplo, si se realiza una apropiación fraudulenta de una cuenta bancaria, no solo es un hurto, también se están violentando seguridades y suplantación de entidad; es por esta razón que creemos que no es tan simple el tener una tipificación general y sanciones comunes para un delito tan complejo que trae varias ilegalidades inmersas.

Realizando una comparación entre el Código Orgánico Integral Penal y el anterior código penal, como se puede observar en la tabla existente que costa el anexo 1 antes la tipificación tenía la pena privativa de libertad y una sanción económica tratándose de delitos informáticos, con el fin de reparar los daños causados a la víctima, pero ahora el COIP solo se preocupa del castigo al sujeto activo por su actuación proveyendo una pena privativa de libertad dependiendo la gravedad del caso. Consideramos que en el caso de los delitos informáticos la sanción económica, además de la privación de la libertad, es importante.

La tipificación debe ser más rigurosa y concreta para este tipo de delitos, ya que como mencionamos anteriormente por lo general tienen varios actos ilícitos involucrados y la investigación supone el uso de nuevas herramientas y participación de gente especializada, sin dejar de lado que muchas veces se requiere de ayuda de instituciones internacionales para poder llegar al verdadero autor; otra razón por la que esto debe estar tipificado rigurosamente es porque muchas veces el cometimiento de estos actos lo realizan varios ciberdelincuentes, muchos de estos pueden estar o no en el país que se encuentra la persona afectada.

2.1.2. La investigación de los delitos informáticos

La Constitución del 2008 atribuye a la Fiscalía la facultad para la intervención de las respectivas investigaciones durante un proceso, como la principal responsable al momento de existir algún delito. El artículo 195 establece que:

> “La Fiscalía dirigirá, de oficio o a petición de parte, la investigación pre procesal y procesal penal; durante el proceso ejercerá la acción pública con sujeción a los principios de oportunidad y mínima intervención penal, con especial atención al interés público y a los derechos de las víctimas. De hallar mérito acusará a los presuntos infractores ante el juez competente, e impulsará la acusación en la sustanciación del juicio penal. Para cumplir sus funciones, la Fiscalía organizará y dirigirá un sistema especializado integral de investigación, de medicina legal y ciencias forenses, que incluirá un personal de investigación civil y policial; dirigirá el sistema de protección y asistencia a víctimas, testigos y participantes en el proceso penal; y, cumplirá con las demás atribuciones establecidas en la ley” (Código Integral Penal, Art. 195).

Lo antes mencionado está en concordancia con el artículo 448 del COIP, el cual menciona en su segundo inciso que:

> “El Sistema contará con el apoyo del organismo especializado de la Policía Nacional y personal civil de investigación, quienes llevarán a cabo las diligencias necesarias para cumplir los fines previstos en este Código, ejecutarán sus tareas bajo la dirección de la Fiscalía y dependerán administrativamente del ministerio del ramo” (Código Integral Penal, Art. 448).

La Dirección de Investigaciones de la Fiscalía General del Estado realiza los procesos de investigación de los delitos, con el fin de que su análisis sirva para ayudar o apoyar las decisiones de los fiscales, ya que son quienes están encargados de recopilar todo tipo de evidencia para llevar a cabo un caso. Para realizar estas investigaciones los expertos hacen uso de las distintas herramientas tecnológicas de las que disponen. Esta Dirección encargada de llevar a cabo las investigaciones se encuentra dividida en distintos departamentos que son:

- Gestión de Medicina Legal y Ciencias Forenses
- Gestión de Coordinación con la Policía Judicial
- Gestión Pericial
- Investigaciones Especializadas

El área que nos compete tratar para este trabajo es el de Investigaciones Especializadas. En el año 2010 se incorporó a la Fiscalía profesionales de distintas ramas y se creó el Departamento de Investigaciones y análisis forense.

Este departamento tiene como misión:

> "El apoyo en la investigación y persecución de todo lo relacionado con la criminalidad informática en todos sus espectros, ámbitos tales como: amenazas, injurias, calumnias, pornografía infantil, fraudes en el uso de las comunicaciones e internet, terrorismo informático, etc., a través de medios electrónicos" (Fiscalía General del Estado, 2011, "Departamento de Investigación y análisis forense", párr.1).

Por tanto la Fiscalía cuenta con un departamento que se encarga de la investigación de delitos informáticos, que es relativamente nuevo dentro de la Institución, y tiene que enfrentarse a los grandes retos de avanzar al ritmo de la evolución de las tecnologías de información y comunicación.

Se debe tomar en cuenta que la investigación requiere herramientas tecnológicas especializadas en descubrir pistas, datos, rutas, direccionamientos y otras especificaciones técnicas que contribuyan a determinar los actores de los delitos; además el personal que usa estas herramientas necesariamente deberá ser experto en materia informática e investigación forense, lo cual implica un procedimiento costoso, por lo que sería necesario valorar inicialmente el costo beneficio de realizar estas investigaciones.

2.1.3. Proceso investigativo y actores

El proceso investigativo en el Ecuador para los delitos informáticos no cuenta con un tratamiento diferente, ya que se les trata como cualquier delito penal, así empieza en la fase procesal, en la cual se realizan las respectivas investigaciones.

La investigación de todo delito penal se inicia con una fase de investigación previa, en la que se reunirán los elementos de tipo y convicción; los elementos de tipo son los que constituyen el delito; y los elementos de convicción son las conductas o los actos que se realizaron para cometer el delito. Estas investigaciones sirven para que el fiscal pueda determinar si es necesario formular o no cargos.

Conforme al artículo 581 del COIP, para iniciarse un proceso investigativo puede existir o no una denuncia y en otros casos puede existir un informe de supervisión. El órgano competente para conocer la causa es la Fiscalía, la cual puede solicitar el apoyo de la Policía Judicial.

Toda la investigación que realice la Fiscalía o persona del sistema especializado integral de la investigación o cualquier institución que intervenga en la investigación previa, debe mantenerla en total reserva, excepto para los sujetos involucrados en la investigación (Código Orgánico Integral Penal, Art. 584).

La duración de las investigaciones dependerá del delito que se esté investigando; es decir si la sanción para un delito es de pena privativa de libertad de cinco años, la fase procesal o de investigación tendrá una duración de un año; mientras que para delitos que tienen una pena privativa superior a los cinco años, la duración que tendrá la investigación es hasta de dos años (Código Orgánico Integral Penal, Art. 585).

Al momento de presentarse una investigación se designa el fiscal para dicho caso, quien conduce la investigación. El fiscal debe ser partícipe en las diligencias de la investigación, las cuales pidió para el esclarecimiento de los hechos; con excepción de los casos en que por naturaleza del delito, se

requiera exclusivamente la intervención de la Policía, el grupo de investigadores o del Sistema Especializado Integral de Investigación (Acurio, 2015, pp. 172-173).

La obtención de las evidencias o pruebas tienen mucha relevancia en el momento de investigar cualquier tipo de delito, no solamente los delitos informáticos, ya que estas evidencias son las que ayudarán a determinar la existencia o la inexistencia de un delito como tal. Con la recolección de dichas pruebas se podrá determinar la responsabilidad de quien aparece en un inicio como presunto responsable, toda evidencia deberá ser recolectada en los términos que manda la ley, la cual será útil para que el tribunal logre dar la mejor resolución en el caso (Acurio, 2015, p.173).

El inciso sexto del artículo 454 del COIP determina que: “Toda prueba o elemento de convicción obtenidos con violación a los derechos establecidos en la Constitución, en los instrumentos internacionales de derechos humanos o en la Ley, carecerán de eficacia probatoria, por lo que deberán excluirse de la actuación procesal” (Código Orgánico Integral Penal, Art. 454).

Es necesario mencionar este artículo, ya que dentro del proceso cualquier tipo de prueba obtenida no puede ser válida, es así que si la prueba fue adquirida realizando una violación a los derechos, ya sea del actor o de la víctima no serán consideradas como válidas.

En nuestra legislación se considera como medios de prueba al documento, testimonio y a la pericia. (Artículo 498 del COIP); en este tema el artículo que nos compete con respecto a las pruebas es el inciso sexto del artículo 499 del COIP, el cual menciona que: “Podrá admitirse como medio de prueba todo contenido digital”, respecto a este artículo entenderíamos que todo dato que se encuentre en un medio electrónico servirá como medio probatorio; pero por otro lado tenemos al artículo 500 del mismo código, que da una breve explicación de lo que se deberá entender por contenido digital, y este menciona que: “Es todo acto informático que representa hechos, información o conceptos de la realidad, almacenados, procesados o transmitidos por cualquier medio tecnológico que se preste a tratamiento informático, incluidos los programas

diseñados para un equipo tecnológico aislado, interconectado o relacionados entre sí”(Código Orgánico Integral Penal, Art.500).

En la investigación de campo realizada se ubicó el Centro de Respuestas a Incidentes Informáticos de la Agencia de Regulación y Control de las Telecomunicaciones del Ecuador, el cual se denomina “Ecucert”.

La misión de Ecucert es "Brindar a su comunidad objetivo el apoyo en la prevención y resolución de incidentes de seguridad informática, a través de la coordinación, capacitación y soporte técnico" (Ecucert Centro de respuesta a incidentes informáticos del Ecuador, s.f.).

Entre sus propósitos encontramos:

1) Apoyar técnicamente a su Comunidad Objetivo en la rápida detección, identificación, gestión y recuperación de datos frente a incidentes de seguridad informática.
2) Proporcionar información técnica, especializada y confiable a las autoridades respectivas durante los procesos investigativos relacionados con incidentes de seguridad informática, de acuerdo a las políticas y procedimientos establecidos.
3) Mantener un laboratorio de análisis técnico enfocado a la identificación de actividades maliciosas, análisis forense, recuperación de datos y elaboración de informes técnicos
4) Apoyar a los organismos de seguridad e investigación del Estado para la prevención e investigación de delitos que involucren tecnologías de la información y comunicación (Ecucert Centro de respuesta a incidentes informáticos del Ecuador, s.f.).

ECUCERT es una dependencia en la que los organismos encargados de la investigación de los delitos informáticos se pueden apoyar, ya que al parecer esta institución cuenta con un laboratorio efectivo y el personal se encuentra ampliamente capacitado.

Entre los propósitos más relevantes de ECUCERT encontramos que busca “Establecer y mantener un vínculo fluido y una relación colaborativa con sus

equivalentes en otros países, así como con organismos internacionales involucrados en ciberseguridad" y también espera "Ser el punto de contacto entre el Estado Ecuatoriano y otros equipos de respuesta internacionales en lo que se refiere a la gestión de incidentes de seguridad informática" (Ecucert Centro de respuesta a incidentes informáticos del Ecuador, s.f.).

Mantuvimos una entrevista con uno de sus funcionarios y explico que se encargan de realizar investigaciones sobre delitos informáticos por encargo de la Fiscalía, y que también realizan investigaciones que parten del registro de incidentes de seguridad en su página web.

La ECUCERT, fue creada con la principal idea de prevenir los delitos informáticos y dar a su comunidad objetivo guías y mejores prácticas de seguridad, pero infortunadamente notamos que esta dependencia no tiene la fuerza ni el reconocimiento por parte de las principales Instituciones competentes en delitos informáticos.

Inclusive en su página web se menciona el procedimiento para la calificación de investigación del incidente reportado a través de esta, pero no indica ninguna relación con la Fiscalía u otro organismo facultado por la ley para recibir denuncias.

Por lo antes mencionado y con el fin de validar los datos encontrados de ECUCERT acudimos a otros medios de información, encontrando que esta dependencia no consta en el organigrama del ARCOTEL por lo que no es posible saber si tiene un presupuesto asignado.

2.2. Realidad procesal

Un aspecto fundamental del presente trabajo es conocer la realidad del Ecuador en cuanto al tratamiento de los delitos informáticos, no teóricamente sino en la práctica, por ello nos enfocaremos en la actuación de las instituciones encargadas del tratamiento e investigación e incluso el accionar del personal encargado del proceso para combatir y llegar a una verdadera sanción.

Como es obvio si para cometer este tipo de ilícitos se necesitan herramientas tecnológicas y un mínimo de conocimiento del uso de las distintas tecnologías existentes, para poder realizar la respectiva investigación de estos delitos, también es necesario tener equipos especializados, personal con amplios conocimientos del uso tanto del software y del hardware y más aún personas con conocimientos investigativos de todo tipo de tecnologías. Como sabemos, en el Ecuador existe ya un retraso tecnológico en comparación con otros países, pues de la misma forma, en el campo investigativo donde se implica la tecnología existen grandes falencias.

Otra de las realidades del país es que al momento de suscitarse una infracción de este tipo, que no existe la adecuada preparación tanto de la Fiscalía como de la Policía Judicial. Como ya se mencionó anteriormente, Santiago Acurio (2008, p. 128) considera que, en el orden técnico existen falencias por la razón de que hace falta infraestructura necesaria, la cual es de suma importancia ya que con estos medios se facilitaría la investigación de los cibercrimenes.

El referente autor considera que la falta de equipos y herramientas tecnológicas modernas para combatir esta clase de delitos hace más difícil manejar un proceso en el cual se vea la existencia de una infracción tecnológica. Para la persecución de los Delitos Informáticos de igual manera falta la suficiente formación tanto de Fiscales que dirigirán la investigación como del cuerpo policial, a la vez menciona que falta una preparación por parte de Jueces y Magistrados, para tratar este tema (Acurio, 2015, p.128).

Es claro que si el país no cuenta con los adecuados procesos y herramientas tecnológicas parar combatir estos delitos, se complicará aún más tanto la investigación como el dar una verdadera o adecuada sanción al culpable.

Es necesario que exista una verdadera capacitación tanto al personal que está encargado de realizar las respectivas investigaciones, como a los funcionarios que administran justicia, porque todos necesitan conocer y entender los términos utilizados en el campo tecnológico, ya que como sabemos cada rama de estudio ya sea del derecho o de la tecnología tendrá su jerga lo cual no es siempre entendible para otras personas. Para combatir este tipo de delitos no

solo se necesita entender cada uno de los términos tecnológicos, sino que a la vez se necesita saber o tener claro que para realizar estas investigaciones se requiere procesos adecuados para manejarlos; para esto citare al doctor Acurio quien hace mención que:

> “En la mayoría de los casos los llamados a impartir justicia se ven confundidos con la especial particularidad de estos delitos y los confunden con delitos tradicionales que por se estructura típica son incapaces de subsumir a estas nuevas conductas delictivas que tiene a la informática como su medio o fin” (Acurio, 2015, p. 128).

Es de suma importancia la capacitación al personal, ya que no se puede tomar a la ligera esta problemática que se está suscitando con los delitos de la nueva era, no basta con la existencia de uno o algunos peritos expertos en el tema, ya que todo el personal que interviene ya sea en la investigación como en el proceso, debe estar al tanto y tener conocimiento de estos temas, para que en cualquier momento esté preparado para actuar frente a la existencia de un delito como estos; pues por la naturaleza y complejidad de los mismo no se les puede dar un trato igual a otros delitos que han venido existiendo desde muchos años atrás.

Existen datos estadísticos sobre delitos informáticos que han sido denunciados, desde que el COIP entró en vigencia. En el periodo enero a agosto de 2015 fueron denunciados 1026 delitos en total, los cuales se especificará detalladamente, conforme a la página de la Fiscalía (Fiscalía General del Estado, s.f.).

Tabla 2. Denuncias de delitos informáticos Enero –Agosto 2015

Delito Tipificado en el COIP	Denuncias de Enero – Agosto de 2015
Art.190.- Apropiación fraudulenta por medios electrónicos.	793
Art.229.- Revelación ilegal de base de datos.	19
Art.230.- Interceptación ilegal de datos	34
Art.231.- Transferencia electrónica del activo patrimonial.	40
Art.232.- Ataque a la integridad de sistemas informáticos	47
Art.233.- Delitos contra la información pública reservada legalmente.	2
Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	91

Adaptado de (Boletín de la Fiscalía, s.f.).

Analizando las estadísticas que constan en la Fiscalía, se puede ver que hoy en día en el Ecuador se cometen Delitos Informáticos, y que las personas e instituciones afectadas, ya acuden a la justicia y realizan su denuncia; estas estadísticas nos demuestran que gracias a las reformas que se realizaron para el nuevo código la población entiende que este tipo de delitos son tomados en cuenta, se atienden y que la justicia está preocupándose de esta nueva forma de delinquir.

De acuerdo a estas estadísticas notamos que uno de los delitos más frecuentes en esta rama es el que se encuentra tipificado en el artículo 190 que se trata de la apropiación fraudulenta por medios electrónicos.

Mientras la Fiscalía presenta 1026 denuncias frente a este tipo de delitos, la Unidad de Investigaciones de Delitos Tecnológicos presenta distintas cifras de los delitos investigados, lo que mencionan en esta unidad es que se realizó 722 investigaciones de ciberdelincuencia en el año 2015, conforme al siguiente detalle.

Tabla 3. Delitos asignados a la Unidad de Investigaciones de Delitos Tecnológicos para su investigación.

Delito	Casos
Apropiación ilícita	340
Publicación, utilización o trasferencia de datos personales sin autorización	210
Análisis Facebook/correo electrónico/ análisis telefónico (Hackeo, virus, spam)	44
Difusión de información falsa por internet	40
Desaparición/ localización	45
Acoso sexual	19
Pornografía infantil	11
Violación de claves o sistemas para acceder u obtener información protegida contenida en sistemas	13

Tomado de (Ministerio del Interior Policía Nacional del Ecuador Dirección Nacional de la Policía Judicial e Investigaciones, s.f.).

Respecto a los delitos mencionados en la tabla, no podemos saber si dichos ilícitos tuvieron una solución para las víctimas, por otro lado no sabemos si ya existen sentencias de los casos, ya que no se pudo realizar un seguimiento de estos casos.

Al realizar una comparación entre los delitos denunciados en la Fiscalía y los delitos que fueron investigados por la Unidad de Investigaciones de Delitos Tecnológicos, notamos que existe una gran cantidad de delitos que no fueron investigados; conforme a las estadísticas 254 delitos no fueron atendidos y no se les administró justicia.

Haciendo una revisión más profunda acudimos a la Unidad referida, que se encuentra ubicada en Quito (Ver Anexo 2 – Tabla de entrevistas); el jefe del departamento nos indicó, que no todos los delitos son asignados para su investigación, ya sea por su naturaleza o por que la Fiscalía los clasifica como

otro tipo de delito; es necesario indicar que esta Unidad trabaja muy confidencialmente y por esta razón no se pudo obtener mayores detalles.

En la investigación de campo realizado se pudo constatar que el tema de delitos informáticos aun es confuso, para algunos funcionarios de las distintas instituciones a donde se acudió a pedir información; por otro lado cabe señalar que este tipo de delitos tiene un tratamiento más confidencial que los delitos comunes.

En la Fiscalía pudimos revisar que no existe una dependencia dedicada a delitos informáticos; en la Fiscalía ubicada en la calle Vicente Ramón Roca nos indicaron que los casos de denuncias de delitos informáticos son distribuidos entre los diferentes departamentos de acuerdo a su tipo.

Esto es una problemática que podemos encontrar en la realidad procesal del Ecuador, ya que no existe un departamento en el que se centralicen este tipo de delitos para llevar los casos. En la entrevista realizada al doctor Santiago Acurio el 16 de mayo del presente año, mencionó que en la actualidad no existe personal experto en el país para llevar este tipo de casos, tanto para la investigación como para administrar justicia. Para Santiago Acurio, es de suma importancia la capacitación al personal en relación con la ciberdelicuencia, porque se debe tener conocimiento detallado de términos propios en relación con la tecnología, ya que la capacitación es clave porque al momento de suscitarse un cibercrimen se realizará un informe con las pruebas obtenidas y tanto el fiscal como los mismos abogados tendrán acceso a este, pero por los términos utilizados que se encuentran en el campo de la informática les será difícil el entendimiento, es por esta razón que todos los involucrados deben tener conocimiento al respecto para poder sobrellevar el caso y poder impartir justicia.

Es evidente que la Fiscalía debe buscar la forma de dar una mejor capacitación al personal respecto a la ciberdelinciencia, ya que es un tema que no solo está ligado con el derecho, sino que está ligado con la informática, lo que complica aún más la preparación del personal.

Sentimos que es necesario que el país cuente con personal capacitado no solamente que realice las investigaciones sino que también es importante que jueces y magistrados se capaciten.

La necesidad de esta capacitación es más evidente al acudir a distintas instituciones relacionadas a delitos informáticos ya que nos pudimos dar cuenta que no existe conocimiento acertado por parte del personal pues al pedir información de cómo se interviene al momento de presentarse un cibercrimen en la Policía Judicial, ubicada en la av. Granados, no supieron dar información al respecto y nos mencionaron que tal vez en la Fiscalía ubicada en la calle Vicente Ramón Roca nos puedan dar información; y al preguntar a otro funcionario de la misma unidad lo que supo indicar es que ahí no se atienden esa clase de delitos y que si necesita más información al respecto deberíamos acudir a la Policía Judicial ubicada en la Av. Eloy Alfaro.

2.3 Retos y desafíos

Uno de los retos que tiene la Fiscalía es implementar una Unidad Especializada Contra la Ciberdelincuencia, con personal que tenga las capacidades técnicas y jurídicas, para que pueda enfrentar cualquier tipo de investigación en relación a delitos informáticos; a través de esta unidad será posible la interceptación de información que circula a través del internet. (Fiscalía General del Estado, s.f.). Esto no implica prescindir de ECUCERT, pues un first responder es indispensable en una sociedad como la actual, que a diario enfrenta potenciales conductas criminales.

El objetivo que se plantea la Fiscalía al tener una unidad especializada para estos delitos, es interesante y a la vez un gran avance no solamente para las investigaciones y su eficacia, sino que será un adelanto para el país en general; contaríamos con equipos especializados y personal con capacidad de para realizar las investigaciones acertadamente y en menor tiempo.

El siguiente desafío al que se enfrenta la Fiscalía en relación a estos delitos es lograr una verdadera capacitación de especialización al personal de las instituciones que intervienen en estos procesos.

Sin embargo el país como tal debe encontrar la manera más ágil y acertada de manejar los delitos informáticos en cuanto a las Instituciones, ya que se debe descubrir si se necesita una administración de justicia centralizada para los delitos informáticos o es mejor como en la actualidad que existe dispersión de las instituciones ligadas a la intervención en la ciberdelincuencia.

Como se ha evidenciado en el presente trabajo no existe una fuente fidedigna y completa con datos sobre delitos informáticos, por lo que se requiere la creación de un repositorio que permita mantener y analizar la información de las denuncias, investigaciones y resoluciones, con el fin de que la población pueda obtener datos precisos en cuanto a ciberdelitos se refiere.

El país se ve retado también a ofrecer fuentes de información que permitan prevenir de los riesgos que existen al momento de hacer uso de las tecnologías de información y comunicación.

Las instituciones facultadas para la intervención en delitos informáticos tienen el gran reto de socializar la información y tratamiento que se da a los delitos en cuestión.

Finalmente, un reto muy importante para el país es lograr formalizar la creación de una entidad como el ECUCERT, ya que tiene el perfil que podría ayudar efectivamente a calificar la importancia de los delitos informáticos, y realizar las gestiones investigativas ya que al pertenecer a una entidad de regulación y control de las telecomunicaciones tiene acceso a realizar seguimientos de la trazabilidad de los actos dentro de las redes informáticas.

Conclusiones

El Ecuador es parte de un mundo globalizado que ha sido impactado por las tecnologías de información y comunicación en todas sus dimensiones. La sociedad de hoy precisa de las TIC para desarrollar el quehacer social, lo cual ha traído múltiples beneficios pero también riesgos y problemas, que en el ámbito penal se traducen en los denominados delitos informáticos o ciberdelitos.

El país respondió con prontitud a la nueva fenomenología criminal que ya era latente en la década de los ochenta. Mediante la reforma introducida por la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, en el 2002 se tipificaron una serie de conductas, que doctrinariamente se correspondían con los delitos informáticos. El actual Código Integral Penal tipificó nuevas conductas, reformó otras y eliminó algunas. Esto evidencia que en cuanto a la criminalización primaria el Ecuador ha sido eficaz.

Sin embargo, desde el 2012 ha sido muy difícil ser efectivos en la criminalización secundaria, esto es llevar a cabo las investigaciones necesarias que permitan sancionar las conductas tipificadas. Esto se puede explicar por la complejidad que representan los delitos informáticos para su investigación y posterior sanción.

El proceso investigativo de los delitos informáticos no es similar al de un delito común. Se requiere personal especializado, tecnología específica y la participación coordinada entre países.

Entonces, la aspiración que tiene la Fiscalía de tener una Unidad Especializada en delitos informáticos se traduce en un imperativo. Pero en cualquier caso se deberá trabajar coordinadamente con todas las instituciones ligadas a la prevención e investigación y los distintos actores deberán contar con las herramientas necesarias, lo que supone una inversión económica importante e indispensable.

Debido a que la investigación de los delitos informáticos es altamente especializada, el personal de las instituciones que participan en el proceso investigativo debe tener igualmente una formación y capacitación especializada. Pero la capacitación debe extenderse también a los jueces y magistrados quienes deben estar al tanto de los términos y de los métodos y medios utilizados al cometer el ilícito, que se utilizan en esta clase de delitos.

Además, Ecuador necesariamente debe tener convenios con distintos países para que le sea más fácil combatir este tipo de delitos. Un paso importante sería ratificar el Convenio de Budapest e integrarse a cualquier iniciativa de la INTERPOL y Naciones Unidas sobre el tema.

Finalmente, Ecuador tampoco cuenta con medidas de prevención para que los ciudadanos sean cuidadosos y responsables en el uso de las TIC, aunque la creación de ECUCERT es un paso importante para lograr activar la reacción ciudadana frente a un delito informático.

REFERENCIAS

Acurio, S. (2007). Delitos Informáticos: Generalidades. *Organización de los Estados Americanos.* Recuperado el 15 de Noviembre de 2015 de http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Acurio, S. (2007). Plan Operativo de creación de la Unidad de Delitos Informáticos del Ministerio Público. *Organización de los Estados Americanos.* Recuperado el 11 de enero de 2016 de http://www.oas.org/juridico/spanish/cyb_ecu_plan_operativo.pdf

Acurio, S. (2015). *Derecho Penal Informático.* Quito, Ecuador: CEP

Altmark, D y Molina, E. (2012). Delitos Informáticos. *Tratado de derecho informático.* Buenos Aires, Argentina: Tucumán.

CCN-CERT Centro Criptológico Nacional. (s.f.). Se impulsa una Fiscalía Especial para luchar contra la criminalidad cibernética. *Diario Jurídico*. Recuperado el 02 de mayo de 2016 de https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/529-se-impulsa-una-fiscalia-especial-para-luchar-contra-la-criminalidad-cibernetica.html

CCN-CERT Centro Criptológico Nacional. (s.f.). El 95% de los ciberdelitos cometidos quedan impunes. *Defensa Frente a la Criberamenaza*. Recuperado el 02 de mayo de 2016 de https://www.ccn-cert.cni.es/seguridad-al-dia/noticias-seguridad/1817-el-95-de-los-ciberdelitos-cometidos-quedan-impunes.html

Código Orgánico Integral Penal, Registro Oficial 180 del 10 de febrero de 2014 y Registro Oficial 180, Suplemento, de 21 de enero de 2016

Constitución de la República del Ecuador, Registro Oficial 449 de 20 de octubre de 2008 y Registro Oficial 490, Suplemento, de 13 de julio de 2011.

Cuenca, A. (2012). *El Delito Informático en el Ecuador "Una nueva tendencia criminal del siglo XXI" su evolución, punibilidad y proceso penal.* Recuperado el 22 de noviembre de 2015 de http://www.egov.ufsc.br/portal/sites/default/files/el_delito_informatico_en_el_ecuador_una_tendencia_criminal_del_siglo_xxi-alexander_cuenca.pdf

Davara, M. (2008). *Manual de Derecho Informático* (10.a ed.). Madrid, España: Aranzadi.

Ecucert Centro de Respuesta a Incidentes Informáticos del Ecuador. (s.f.). *Centro de Respuestas a Incidentes Informáticos del Ecuador.* Recuperado el 20 de mayo de 2016 de https://www.ecucert.gob.ec/proceso.html#ANCHOR_Box1

Ferruzola, E., y Cuenca, H. (2014). Cómo responder a un Delito Informático. Revista Ciencia Unemi. Vol. N. 11, 43 - 50. Recuperado el 18 de enero de 2016 de http://www.unemi.edu.ec/ojs/index.php/cienciaunemi/article/viewFile/111/112

Fiscalía General del Estado. (s.f.). *Investigaciones.* Recuperado el 09 de abril de 2016 de http://www.fiscalia.gob.ec/index.php/sala-de-prensa/boletines-2011/31

Fiscalía General del Estado. (s.f.). *Tenga cuidado!, con un solo 'clic' podría caer*

en la red de los delitos informáticos. Recuperado el 30 de abril de 2016 de http://www.fiscalia.gob.ec/index.php/sala-de-prensa/4229-%C2%A1tenga-cuidado-,-con-un-solo-clic-podr%C3%ADa-caer-en-la-red-de-los-delitos-inform%C3%A1ticos.html

Fiscalía General del Estado. (s.f.). *23 nuevos fiscales provinciales se posesionaron en sus cargo.* Recuperado el 30 de abril de 2016 de http://www.fiscalia.gob.ec/index.php/sala-de-prensa/4246-40-funcionarios-de-fiscal%C3%ADa-participaron-en-taller-para-investigar-ciberdelitos.html

Fiscalía General del Estado. (s.f.). *Los delitos informáticos van desde el fraude hasta el espionaje.* Recuperado el 16 de enero de 2016 de http://www.fiscalia.gob.ec/index.php/sala-de-prensa/3630-los-delitos-inform%C3%A1ticos-van-desde-el-fraude-hasta-el-espionaje.html

Ministerio del Interior de España. (s.f.). *Cibercriminalidad*. Recuperado el 19 de abril de http://www.interior.gob.es/documents/10180/1207668/Avance+datos+ciberciminalidad+2013.pdf/5de24ec6-b1cc-4451-bd06-50d93c006815

Ministerio del Interior Policía Nacional del Ecuador Dirección Nacional de la Policía Judicial e Investigaciones. (s.f.). *Unidad de Investigación de Delitos Tecnológicos.* Recuperado el 21 de mayo de 2016 de http://www.portal.dnpj.gob.ec/inicio/images/DOC_PUB/TRANSPARENCIA/2015/INFORME%20DE%20RENDICION%20DE%20CUENTAS%20DNPJeI-2015.pdf

Naciones Unidas. (s.f.). *Delitos Informáticos. Oficina contra la Droga y el Delito*. Vol. N. 05. Recuperado el 01 de abril de 2016 de http://www.unis.unvienna.org/pdf/05-82113_S_6_pr_SFS.pdf

Observatorio de Ciberseguridad en América Latina y el Caribe. (s.f.). *Ciberseguridad ¿Estamos preparados en América Latina y el Caribe*. Recuperado el 21 de mayo de 2016 de http://observatoriociberseguridad.com/graph/countries//selected//0/dimensions/1-2-3-4-5

Rebolo, J. (2009). Los delitos Informáticos. *Boletín Criminolóxico*. Vol. N. 11. Recuperado el 05 de noviembre de 2015 de https://www.usc.es/export/sites/default/gl/institutos/criminoloxia/descargas/Los_Delitos_Informxticos.pdf

Smartekh. (s.f.). La Historia del Cibercrimen. Grupo Smartekh. Recuperado el 29 de abril de 2016 de http://blog.smartekh.com/la-historia-del-cibercrimen/

Téllez, J. (s.f.). *Derecho Informático*. Recuperado el 01 de abril de 2016 de http://biblio.juridicas.unam.mx/libros/1/313/5.pdf

Verne,V. (s.f.). Informática Forense y su Realidad Procesal en el Ecuador. *Informatica Forence, Inserción Jurídica*. Recuperado el 20 de abril de 2016 de http://repositorio.utn.edu.ec/bitstream/123456789/539/9/04%20ISC%20157%20CAPITULO%20IV.pdf

ANEXOS

ANEXO 1

Conductas tipificadas en el Código Penal derogado por Ley 180 de 10 de febrero de 2014

Delito	Pena Privativa de Libertad	Sanción Económica
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. Si la información obtenida se refiere a seguridad nacional, o a secretos comerciales o industriales. La divulgación o la utilización fraudulenta de la información protegida, así como de los secretos comerciales o industriales.	Reprimido con prisión de 6 meses a 1 año. Pena de reclusión 1 a 3 años. Pena de reclusión de 1 a 6 años	Multa de 500 a 1000 dólares Multa de 1000 a 500 dólares. Multa de 2000 a 10.000 dólares
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.	Pena de prisión de 2 meses a 2 años.	Multa de 1000 a 2000 dólares
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.	Reprimidos con 3 a 6 años.	
Daños informáticos.- El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de	Reprimido con prisión de 6 meses a	Multa de 60 a 150 dólares

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	3 años	
Apropiación ilícita.-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.	Reprimidos con prisión de 6 a 5 años	Multa de 500 a 1000 dólares
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.	Pena de prisión de 1 a 5 años	Multa de 1000 a 2000 dólares
La destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos	Reprimida con prisión de 8 meses a 4 años.	Multa de 200 a 600 dólares
Quien produjere, publicare o comercializare imágenes pornográficas, materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato, u organizare espectáculos en vivo, con escenas pornográficas en que participen los mayores de catorce y menores de dieciocho años.	Reclusión de 6 meses a 9 años, comiso de objetos y de bienes producto del delito	

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.	De conformidad con lo establecido para los otros delitos establecidos en el Código Penal	

ANEXOS 2

Entrevistas Realizadas

Nombre	Unidad	Dirección	Extracto de la Información
Ricardo Muñoz	Unidad de Investigaciones de Delitos Tecnológicos de la Policía Nacional	Av. Amazonas y Vicente Ramón Roca	El jefe del departamento indicó que no todos los delitos informáticos les son asignados para su investigación ya que muchos delitos denunciados, la Fiscalía no les da la naturaleza de delito informático. Por otro lado el funcionario mencionó que la información que manejan en su unidad es clasificada como confidencial y no se nos puede proporcionar más datos.
Patricio Culquicondor		Calle Vicente	La información proporcionada fue que no existe un departamento específico para tratar delitos

	Fiscalía	Ramón Roca	informáticos en general, sino que dependiendo el bien jurídico protegido, se le envía a la unidad competente. También se le pregunto de cómo es la relación de trabajo con Ecucert, pero el funcionario menciono que no sabe de la existencia de dicha unidad.
Dr. Santiago Acurio	Sala Penal de la Corte Provincial de Pichincha	Av. 6 de Diciembre – Plaza Argentina	El doctor Acurio supo dar una explicación de los procesos y la complejidad que existe al momento de presentarse un delito informático e hizo mención sobre la falta de capacitación para funcionarios competentes que manejan este tipo de delitos.
Franklin Álvarez	Ecucert	Av. Amazonas N40-71 y Gaspar de Villaroel	Unidad perteneciente o vinculada a ARCOTEL; el agente de seguridad de Ecucert menciona que cualquier persona que haya sido afectada mediante un delito informático primero debe acudir a realizar su denuncia en Fiscalía y que posteriormente si alguna de las unidades que realiza la investigación solicita el apoyo Ecucert presta sus servicios. Indicó también que los principales usuarios de sus servicios son las empresas de comunicaciones.
Dra. Elsa Moreno	UDLA	Calle José Queri	La doctora Moreno dio una explicación detallada del proceso de investigación de los delitos, tomando como punto de inicio del proceso la denuncia presentada por los afectados.
Recepción	Policía Judicial	Av. Granados	Uno de los funcionarios no supo dar información, y nos remitió a la Fiscalía antes ya mencionada; otro funcionario de la misma unidad mencionó que ahí no se atienden delitos

			informáticos.
Prevención	Dirección Nacional de la Policía Judicial	Av. Eloy Alfaro	Nos indicaron que los datos sobre delitos informáticos se manejados de forma reservada y no se nos puede proporcionar información.