REPÚBLICA DEL ECUADOR

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
LA UNIVERSIDAD DE POSTGRADO DEL ESTADO

Maestría en Derecho Procesal Penal y Litigación Oral

Trabajo de titulación previo a la obtención del título de
Máster en Derecho Procesal Penal y Litigación Oral

Tema:

Articulación de la Fiscalía General del Estado para la persecución de delitos cibernéticos

Autor: Hugo Alexander Cuenca Espinosa
Tutor: Natalia Alejandra Mora Navarro

Quito, abril 2022

INSTITUTO DE ALTOS ESTUDIOS NACIONALES
LA UNIVERSIDAD DE POSGRADO DEL ESTADO

No.488 - 2022.

ACTA DE GRADO

En el Distrito Metopolitano de Quito, hoy 06 de julio de 2022, **HUGO ALEXANDER CUENCA ESPINOSA,** portador del número de cédula: 1721047551, **EGRESADO DE LA MAESTRÍA EN DERECHO PROCESAL PENAL Y LITIGACIÓN ORAL (2021-2022),** se presentó a la defensa del Artículo Cientifico, con el tema, **"ARTICULACIÓN DE LA FISCALÍA GENERAL DEL ESTADO PARA LA PERSECUCIÓN DE DELITOS CIBERNÉTICOS"**, dando así cumplimiento al requisito, previo a la obtención del título de **MAGÍSTER EN DERECHO PROCESAL PENAL Y LITIGACIÓN ORAL.**

Habiendo obtenido las siguientes notas:

Promedio Académico:	8.83
Artículo Cientifico:	9.07
Defensa Oral Artículo Cientifico:	9.50
Nota Final Promedio:	**9.05**

En consecuencia, **HUGO ALEXANDER CUENCA ESPINOSA,** se ha hecho acreedor al título mencionado.

Para constancia firman:

Mgs. Milton Rocha
PRESIDENTE

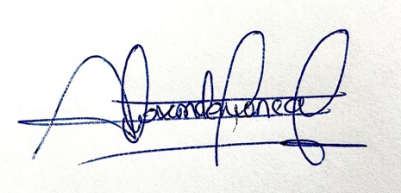
Dr. Tomás Sánchez
MIEMBRO

Dr. Alex Valle
MIEMBRO

Abg. Juan Maldonado.
DIRECTOR DE SECRETARÍA GENERAL

AUTORÍA

Yo, Hugo Alexander Cuenca Espinosa, cédula de ciudadanía 172104755-1, declaro que las ideas, juicios, valoraciones, interpretaciones, consultas bibliográficas, definiciones y conceptualizaciones expuestas en el presente trabajo, así como los procedimientos y herramientas utilizadas en la investigación, son de absoluta responsabilidad de el autor del trabajo de titulación. Asimismo, me acojo a los reglamentos internos de la universidad correspondientes a los temas de honestidad académica.



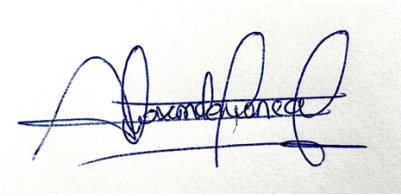
HUGO ALEXANDER CUENCA ESPINOSA

C.C. 172104755-1

AUTORIZACIÓN DE PUBLICACIÓN

Autorizo al Instituto de Altos Estudios Nacionales (IAEN) la publicación de este trabajo de titulación, de su bibliografía y anexos, como artículo en publicaciones para lectura seleccionada o fuente de investigación, siempre dando a conocer el nombre del autor y respetando la propiedad intelectual del mismo.

Quito, 12 de abril de 2022



HUGO ALEXANDER CUENCA ESPINOSA

C.C. 172104755-1

DEDICATORIA

A Karina Elizabeth, mi compañera incansable.

A Constanza Alessandra, mi regalo de Dios.

AGRADECIMIENTO

A mis padres por siempre creer en mí. A mi esposa por siempre apoyarme.
A mis amigos y colaboradores por ver en mí un ciudadano ejemplo de la sociedad.

Articulación de la Fiscalía General del Estado para la persecución de delitos cibernéticos

Una aproximación de la teoría a la práctica

RESUMEN

El presente artículo estudia los mecanismos de cooperación y aplicación que tiene la Fiscalía General del Estado del Ecuador para la investigación de los delitos cibernéticos, partiendo de los acuerdos interinstitucionales que hacen posible la persecución y esclarecimiento de estos delitos, hasta un análisis de los principales convenios internacionales en la materia de los cuales el Ecuador es partícipe. Este trabajo conlleva un estudio teórico-práctico de los ciberdelitos, que aborda tres aristas muy importantes, por un lado, un estudio doctrinario, por otro, una investigación de campo basada en entrevistas a los principales protagonistas del tema en instituciones públicas y, finalmente, una serie de comentarios y experiencias del autor sobre el estudio de la temática por más de diez años.

Palabras clave: delitos cibernéticos, ciberespacio, cooperación penal internacional, fiscalía, crimen organizado, derecho penal, criminalidad informática.

ABSTRACT

This article studies the mechanisms of cooperation and application that the Attorney General of the State of Ecuador has for the investigation of cybercrimes, starting from the interinstitutional agreements that make possible the prosecution and clarification of these crimes, up to an analysis of the main agreements international agreements in which Ecuador is a participant. This work entails a theoretical-practical study of cybercrimes, which addresses three very important aspects, on the one hand, a doctrinal study, on the other, a field investigation based on interviews with the main protagonists of the subject in public institutions and, finally, a series of comments and experiences of the author on the study of the subject for more than ten years.

Keywords: cybercrime, law enforcement, crime unit, cyberspace, criminal cooperation, criminal prosecutor, organized crime, criminal law.

ÍNDICE

ÍNDICE DE GRÁFICOS

1. Introducción

Como advertencia previa a la investigación del tema objeto de este trabajo de titulación, debo mencionar que su complejidad radicó en cinco puntos: 1. En la escases de fuentes bibliográficas sobre el tema; 2. Por la ausencia de investigación en la materia desde el campo de las ciencias criminológicas; 3. En la interpretación conceptual y nominal de la materia; 4. Por la falta de un estudio dogmático de los tipos penales que componen la criminalidad informática como fenómeno delictual; y, 5. Por los secretismos de las instituciones del Estado en brindar información que ayude a mejorar la investigación del presente trabajo.

Haciendo énfasis sobre el cuarto punto, la carencia del estudio dogmático sobre la criminalidad informática recae esencialmente en los elementos de la tipicidad, puntualmente en el verbo rector, sujeto activo y bien jurídico vulnerado, por lo tanto, esta investigación nos plantea una ardua tarea que permite —sin lugar a duda— tener un panorama más claro en lo que respecta al desarrollo académico de esta nueva temática.

Debemos referirnos también que la mayoría de autores —como ya lo veremos *a posteriori*— no hacen una clara diferencia de los diversos conceptos que envuelven a los delitos cibernéticos; así por ejemplo, a todos los delitos cometidos a través de una computadora, los generalizan como delitos informáticos, al fenómeno delictual lo categorizan como cibercrimen, y al modo de proceder del sujeto activo como delincuencia informática. Es claro que el sucinto estudio hecho hasta la actualidad, impide que no destaquen otros aspectos investigativos a profundidad, como los medios, el fin y la naturaleza jurídica de esta temática conforme las políticas criminales presentes.

Como decíamos, el esfuerzo de esta investigación tiene su precio, sustancialmente porque responde a una formulación nueva de la doctrina, en la que se dilucide con claridad conceptos que hasta hoy han sido erróneamente interpretados y definidos, es por esta razón que esta investigación tiene cierto grado de dificultad, sin embargo, el resultado final ha de ser gratificante y enriquecedor para la ciencia penal.

Para concluir, hago mención a Fernando Alfredo Ubiría que en su obra *Reparación de daños derivados del transporte benévolo*, (2004) citado por Jorge Horacio Alterini en lo siguiente “en el Derecho no hay temas agotados, sino autores agotados por los temas” (p. 23), haciendo alusión a este frase, nos espera una larga y ardua tarea, en la que el premio más grande concluirá con la creación de una nueva doctrina capaz de aportar a la ciencia en el campo penal,

fruto del conocimiento, del estudio, de la investigación y del empeño por beneficiar desinteresadamente a un colectivo de la sociedad, denominado Academia.

1.1. Objeto de la investigación, importancia y aporte a la ciencia penal

El objeto del presente trabajo se circunscribe al desarrollar un texto de investigación sobre la articulación que hace la Fiscalía General del Estado (FGE) para perseguir e investigar los ciberdelitos, aplicado a los convenios, tratados y acuerdos con las diferentes instituciones nacionales y extranjeras, tema que ha sido escasamente investigado.

Tiempo atrás los delitos cibernéticos para su consumación se realizaban por particulares o grupos pequeños de hasta tres personas, a diferencia de hoy en que se manejan bajo modalidades de crimen organizado, es fundamentalmente por esta razón que tomamos como objeto de estudio la presente temática, que rige como eje fundamental del saber cómo funciona el aparataje institucional investigativo para esclarecer los delitos tecnológicos, evitando impunidad de estos en la sociedad.

El aporte fundamental de la presente investigación a la ciencia penal, radica en la investigación sobre la articulación que hace la FGE con otros entes para no dejar la mayoría de ciberdelitos en la impunidad como suele pasar. Así también, resulta importante fundamentar y esclarecer varios vacíos conceptuales, puesto que, ayudan a los diferentes entes del quehacer jurídico a entender la materia y los términos técnicos que son de importante preocupación al momento de la aplicación de la ley por parte de jueces y abogados, y de su entendimiento por los lectores y público en general.

Para finalizar este acápite, el aporte doctrinal a la materia conllevará un adecuado entendimiento de la materia penal informática, lo que implicará un mejor desenvolvimiento del derecho en el quehacer diario de quienes ejercen y estudian esta innovadora línea de investigación.

Sin lugar a duda, el presente tema de investigación dejará mucho más claro el panorama del actuar investigativo de los entes que tutelan la acción público penal en el Ecuador, siendo el aporte más importante las líneas o guías que maneja la Fiscalía para la persecución de delitos cibernéticos, hechos clave que todo abogado necesita conocer para coordinar y ayudar a sus clientes en el esclarecimiento de la verdad y la obtención de la tan anhelada justicia.

1.2. Sustento fenomenológico

El fenómeno de la criminalidad informática, envuelve a las conductas típicas y atípicas contrarias al orden social, que toman como principales instrumentos el internet, la computadora y la electrónica, para su comisión o perpetración.

Es menester señalar que el término «delito informático» fue por primera vez utilizado entre las décadas de los ochenta y noventa, en una época en la que se deducía que estos delitos eran meramente resultado del uso de los equipos informáticos, a diferencia de hoy en día en que se sabe que es necesario el uso de otras tecnologías como el "internet" para la consumación de estos, incorporando incluso otros elementos que no han sido acogidos por la doctrina debido a su falta de claridad, entendiéndose una ineficaz investigación en la que se pueda facilitar el uso y aplicación de diversos términos técnicos pertenecientes a esta temática.

Por esta cuestión, la terminología que comprende el derecho penal, de por sí tiene diferentes acepciones que al ser utilizada por dos o más locuciones para expresar un mismo significado —a manera de sinónimo— puede acarrear una errónea interpretación.

Continuando con lo dicho anteriormente, los delitos cibernéticos en principio se llamaron delitos informáticos pues su estrecha relación con la informática y los actos delictivos dieron paso a ese nombre, no obstante, con el pasar del tiempo estos fueron aumentando y evolucionando, de tal manera que, en la actualidad ya no solo se emplea el término «hacker», sino otros nombres derivados de este, haciendo una extensa clasificación entre el tipo de autores, el tipo de delitos, las modalidades criminales, las conductas delictivas, los métodos usados y las herramientas empleadas; además que, la diversificación y conceptualización de estos delitos recae en nuevas clasificaciones como delitos computacionales y electrónicos.

La criminalidad informática como fenómeno de estudio en materia penal, implica dos perspectivas metodológicas: 1) Una perspectiva cualitativa, en base al análisis de datos de la información observada, recopilada e investigada; y, 2) Una perspectiva cuantitativa, en relación a los datos estadísticos obtenidos y proporcionados de los delitos suscitados en el Ecuador.

Aun cuando el derecho penal informático y el derecho informático son dos ramas que no gozan de autonomía propia —por cuanto el primero es visto desde el campo del derecho público al ser parte de la ciencia penal, y el segundo es visto desde el campo del derecho privado al responder a ciertos actos y contratos derivados del internet propios del ámbito civil— lo que se pretende es crear una base sólida, capaz de afianzar al derecho penal informático como un área perteneciente a la ciencia penal parte del derecho público.

Pese a que mucho se ha hablado de los delitos informáticos, poco se ha hecho por investigar el fenómeno y carácter criminológico que los envuelve; partiendo de la escases de

aportes relativos al tema, que puedan sustentar los acontecimientos delictuales que hoy en día son materia de persecución y punibilidad, hasta la falta de normativa plena dentro del derecho positivo en lo que respecta a política criminal.

2. Delitos cibernéticos y derecho penal informático

2.1. Qué son los delitos cibernéticos

Es toda actividad delictiva en la cual se utilizan los sistemas y medios computacionales, telemáticos y electrónicos como medio y fin para la consumación de un delito, que principalmente afectan al dato y a la información como bienes jurídicos protegidos (SEGEN, 2020). Por lo tanto, los delitos cibernéticos constituyen nuevas conductas antijurídicas que incluyen dentro de sus elementos principales al internet como instrumento abstracto y a la computadora como instrumento físico. Los ciberdelitos en sus diferentes tipos y/o facetas son susceptibles de ser sancionados, siempre y cuando la conducta antijurídica se encuentre configurada y establecida en el Código Penal.

2.2. Ciberdelito como medio y fin

Dentro de los llamados ciberdelitos, un tema importarte a resaltar es la manera de cómo son clasificados estos, por lo que los clasificaremos en base a dos criterios: 1) Como medio o instrumento. 2) Como fin u objeto.

De acuerdo a Julio Téllez Valdés (2002), citado en Levene (2002), como instrumento o MEDIO "se tienen a las conductas criminógenas que se valen de las computadoras como método, medio o símbolo en la comisión del ilícito"; mientras que como FIN u objeto "se enmarcan las conductas criminógenas que van dirigidas en contra de la computadora, accesorios o programas como entidad física" (p.15).

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

2.3. Sujeto activo y pasivo en el ciberdelito

a) Sujetos activos

En materia penal se dice que el sujeto activo es "aquella persona que realiza la acción penal prohibitiva u omite la acción penal esperada, que en ciertas circunstancias la ley exige una calidad o condición especial" (Sacoto, 2013, p. 25). En delitos informáticos si hablásemos de

sujeto activo, es el conocido de forma general por la sociedad como “hacker”, quien es la persona con ciertas habilidades para el manejo de sistemas informáticos, y que generalmente por su situación laboral, se encuentra en lugares estratégicos donde se maneja información de carácter sensible, o bien son hábiles en el uso de los sistemas informáticos, aun cuando en muchos de los casos, no desarrollen actividades laborales que faciliten la comisión de este tipo de delitos (Levene, 2002).

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

El problema que respecta en lo relacionado al sujeto activo como ente principal para la comisión de un delito informático, radica en el hecho que la mayoría de ilícitos son cometidos por los llamados “insiders”, pues estos facilitan la comisión del delito y la fuga de información, afectado principalmente al dato como bien jurídico tutelado por el Estado.

b) Sujetos pasivos

Debemos comenzar diciendo que el sujeto pasivo o víctima es la persona o cosa sobre la cual recae la acción antijurídica cometida por el sujeto activo (López, 2020). En materia penal informática, el sujeto pasivo es la víctima del delito informático, sobre la cual recae la acción dolosa producida por el sujeto activo a través de la computadora u objeto telemático con la ayuda de la tecnologías de la información o TIC’s.

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

2.4. Clases de delitos cibernéticos

2.4.1. Diferencia entre delito informático y delito computacional

La evolución de los delitos informáticos, no solo ha mutado en sus técnicas, procedimientos y modos de operar, sino que también ha dado una transformación conceptual, partiendo de este punto, podemos considerar que el computador y sus aplicaciones constituyen el objeto material del delito por lo que podemos estar hablando de Delito Informático, mientras que si se lo considera como un mero instrumento para la comisión de actos que generalmente

están tipificados en el Código Penal lo encasillaríamos como Delito Computacional, es así que para dilucidar la diferencia entre el concepto del Delito Informático y el Delito Computacional, basta en centrarnos y ver a la computadora como un medio y como fin para hacer una mera diferencia entre estas dos acepciones de acuerdo a lo expuesto por Romero Casabona (1987).

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

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

2.5. Aproximación a la criminalidad informática: Nociones preliminares

A partir de los años sesenta, la humanidad dio paso al descubrimiento y desarrollo de la tecnología; en principio no fue de libre acceso al público, puesto que, por su infraestructura física —en el caso de las computadoras— y su alto costo, imposibilitaban que una persona cualesquiera pueda tener acceso a esta.

Con el avance tecnológico, el ser humano logró automatizar tiempo y recursos, ya que con el empleo de la llamada Inteligencia Artificial o por sus siglas en inglés *AI*, se podía hacer una actividad específica —aunque simple— sin la intervención de la persona, es así que con máquinas desarrolladas, de gran potencia y magnitud, se reemplazaba parcialmente el trabajo físico e intelectual del ser humano.

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

El problema radica en que la tecnología no siempre ha sido usada con un fin benévolo, puesto que ciertas personas —autodenominados hackers— han abusado de esta para actos

maliciosos y de satisfacción personal, utilizando este recurso para la comisión de ilícitos informáticos; esto nos lleva a pensar acertadamente que la conducta de ciertos individuos esta inclinada hacia la comisión de delitos y a la satisfacción de pretensiones personales de carácter pecuniario, a toda costa; como resultado de estas nuevas formas de delinquir —distintas de las convencionales— y con el desarrollo de la informática aparecen los llamados *delitos informáticos.*

Según Levene (2002), nos dice:

> El delito informático implica actividades criminales que un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraudes, falsificaciones, perjuicios, estafa, sabotaje, etc., sin embargo, debe destacarse que el uso indebido de las computadoras es lo que ha propiciado la necesidad de regulación por parte del derecho de estos actos para evitar la impunidad (p. 35).

2.6. La naturaleza jurídica de la criminalidad informática y de los delitos cibernéticos

El axioma de la naturaleza jurídica de un delito informático es un hecho jurídico (Astigueta, 2016), puesto que los múltiples comportamientos irregulares que se dan con el avance de la tecnología, determinan diferentes conductas que permiten la comisión del delito, es por eso que se vuelve necesario buscar la forma o método para hacer de estas conductas un hecho punible.

Los Delitos Informáticos en su mayoría son delitos tradicionales que con la ayuda de la TIC's suponen nuevas formas de delinquir, que conllevan en ciertos casos a la creación de nuevos tipos penales, y de una nueva conceptualización sobre la tendencia criminal, a su vez deriva en una nueva aplicación del principio de territorialidad por el cometimiento de estos en el medio -espacio- digital; así como Posada (2017) determina que los cibercrímenes con características particulares interviene la acción, el sujeto, el resultado y la imputación, variables que hacen replantear y modificar la línea de investigación en el ciberdelito.

Debemos acotar que la naturaleza jurídica de los delitos cibernéticos, están encaminada al sustento fenomenológico del campo del derecho, tanto desde su parte conceptual o teórica como su parte práctica, se debe entender que las características propias de este tipo de delitos se basan en contextos y sujetos que intervienen en el caso.

Así pues, en el hecho se identifica al sujeto activo quien comete la acción (hacker, phreaker, cracker, etc.), y al sujeto pasivo en quien recae la acción antijurídica (víctima), los parámetros que conlleva el verbo rector sobre la acción antijurídica realizada (obtener, clonar, adulterar, acceder, etc.) y los elementos base -fácticos- con los que pretende probar los enunciados, hipótesis y teorías (redes sociales, internet, computador, dispositivos electrónicos, etc.).

Ahora bien, los perpetradores de los ciberdelitos en su mayoría se los distingue por ciertas particularidades como, los dogmas y reglas de status, seudónimos, costumbres poco vistas, el tipo de religión como budismo o taoísmo, su elevado coeficiente intelectual y más, de acuerdo a Rivera (2009).

2.7. Planteamiento actual de los ciberdelitos

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

Entre las definiciones más conocidas podemos destacar a Julio Téllez Valdés (2002), quien en su obra *Derecho Informático* plasma el concepto de Delito Informático desde dos acepciones, la primera como forma típica entendiendo a *"*las conductas típicas, antijurídicas y culpables en que se tienen a las computadoras como instrumento o fin, [y la segunda como forma atípica, entendiendo a] las actitudes ilícitas en las que se tiene a las computadoras como instrumento o fin" (p. 60).

Así mismo se destaca el concepto de Callegari (2016), quien define al Delito Informático como "aquel que se da con la ayuda de la informática o de técnicas anexas" (p. 25), entendiendo como técnicas anexas, a las formas de utilizar las técnicas del hacking para la comisión de ilícitos. Hay que precisar que, este concepto no es del todo claro, pues la tratadista sólo toma la informática como medio para la consumación del delito y no como objeto de la infracción.

Por otro lado, el Departamento de Investigación de la Universidad de México, señala como delitos informáticos a "todas aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, que hacen uso indebido de cualquier medio Informático" (Viega, 2011, p.35).

Carlos Sarzana (2014), define el Delito Informático como "cualquier comportamiento criminógeno en que la computadora está involucrada como material, objeto o mero símbolo" (p.52).

María de la Luz Lima, quien dice que el delito electrónico en su sentido amplio es:

> Cualquier conducta criminógena o criminal que en su realización hace uso de la tecnología electrónica ya sea como método, medio o fin y que, en un sentido estricto, el delito Informático, es cualquier acto ilícito penal en el que las computadoras, sus técnicas y funciones desempeñan un papel ya sea como método, medio o fin (De la Luz, 2014, p. 56).

Se puede considerar que dentro de este concepto, lo que trata la autora es de hacer una pequeña, pero clara diferencia entre lo que es un delito electrónico y un delito informático, confundido casi siempre por la ambigüedad del término, ya que no se hace una distinción entre

el delito informático y el delito computacional, puesto que el delito informático ataca a la información y al dato como bienes jurídicos protegidos, mientras el delito computacional utiliza a la computadora como medio para la comisión del delito, y como objeto de la infracción.

Renato Jijena Leiva (1992) 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" (p. 225).

Por el lado ecuatoriano, tenemos a Santiago Acurio del Pino (2010), quien realiza un aporte importante al mencionar que sin circunscribirse a términos rígidos como delitos informáticos, hace hincapié en el término delincuencia informática para referirse a ellos, indicando que este es:

> Todo acto o conducta ilícita e 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 (Acurio, 2010, p.180).

A la vez Acurio del Pino (2010), destaca que parte importante de la doctrina señala:

> Que no estamos frente a nuevos delitos, sino más bien ante una nueva forma o formas de llevar a cabo los delitos tradicionales, por lo que no vale individualizarlos de una manera específica, correspondiendo al legislador introducir las modificaciones legales pertinentes a fin de adecuar los tipos penales tradicionales a los nuevos modos de proceder por parte de delincuentes (Acurio, 2010, pp. 177-178).

De esta manera, reduciríamos el excesivo número de tipos penales que existen en la legislación ecuatoriana, adaptando al delito tradicional las nuevas formas de delinquir, que en la actualidad hacen uso de la tecnología como su herramienta de trabajo; y lo más importante partiendo del hecho que, más allá de los mecanismos usados para la comisión del delito, está la vulneración del bien jurídico protegido, dando importancia primordial a la información y al dato, mas no exclusividad, pues tenemos otros bienes jurídicos que pueden ser afectados como la seguridad nacional, la intimidad personal, la integridad sexual, el patrimonio, etc.

A esta conclusión, se une el concepto de Enrique Rovira del Canto (2004), citado en González (2004) quien menciona que el delito informático:

> No debe venir referido a la realización de una conducta ilícita a través de elementos o medios informáticos, meramente que éstos sean objeto de tal comportamiento delictivo, sino que debe constituirse en torno a la afectación de la información como bien jurídico protegido, primordial y básico, que no exclusivo. Por tanto, se deberá tener presente si resultan afectados otros bienes jurídicos, normalmente tradicionales (González, 2004, p. 71).

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

2.8. Dimensión del problema delictual y problema jurídico en el contexto nacional

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

Por otro lado, existe el desconocimiento de esta área por parte del legislador a la hora de tipificar estas conductas penales, ya que al desconocer de la materia, no se puede tipificar con lucidez ciertos actos, que por su constitución entre lo técnico y lo legal, son diferentes a la mayoría de delitos, tanto en su verbo rector, como en los sujetos procesales intervinientes. Sobre la tipificación de la norma, los tipos penales relativos a delitos informáticos poseen ciertos vacíos legales, que al aplicarlos a casos concretos —sobre todo en el área de criminalidad informática— pueden ser indebidamente interpretados por los entes judiciales, puesto que, además de ser estar dentro del ámbito jurídico, como ya lo mencionamos anteriormente, poseen también un contexto técnico.

La incorrecta interpretación de la norma y aplicación de la ley, acarrea varios problemas, uno de ellos puede ser un resultado inesperado por parte del accionante a la hora de obtener justicia, o un resultado desfavorable para el procesado, en caso que se le imponga una pena distinta al acto cometido. Este problema a su vez, está ligado a una falta de profesionales —como jueces y fiscales— afines a la materia penal informática, que puedan de manera aplicar la correspondiente sanción normativa o disponer del respectivo dictamen acusatorio en el momento de la audiencia por esta clase de ilícitos. Esta falta de capacitación conlleva a que tanto jueces como fiscales no puedan comprender, juzgar, investigar y aplicar la correspondiente sanción penal —en el caso de jueces— por este tipo de actos.

En el caso ecuatoriano, además de la errónea interpretación de los tipos penales, la problemática clave desde el objeto de investigación radica en que no existen los lineamiento por parte de la Fiscalía General del Estado para perseguir e investigar los delitos cibernéticos, más bien todo se lo hace de manera consuetudinaria, lo que resulta que los requerimientos y respuestas a estos sean mecánicos y poco observados, esto trae como consecuencia que no se haga una investigación totalmente proba, no se obtengan los elementos de convicción y conocimiento necesarios para avanzar en el proceso penal, lo cual a su vez crea indefensión e

impunidad sobre la víctima, y, finalmente, cause retrasos en la obtención de justicia y el acceso a la misma.

Es la inclusión de fiscalías especializadas en el tema, que, además de la capacitación a jueces y fiscales para que tengan mayor conocimiento sobre este tipo de delitos, puedan proveer la seguridad jurídica necesaria en sus actos, condición *sine qua non que* todo estado de Derecho necesita para el cumplimiento de los principios y normas consagradas en la Constitución, la Ley y Tratados Internacionales.

Para concluir este punto, podemos tomar como referencia el sistema judicial en la Argentina, que posee fiscalías especializadas en delitos tecnológicos, con fiscales de amplia experiencia en la materia como Daniela Dupuy, quien es Fiscal de la Unidad Fiscal Especializada en Delitos y Contravenciones Informática de la ciudad de Buenos Aires, persona de renombre que posee una alta capacidad y conocimiento de la materia penal informática en la República de la Argentina.

2.9. Conclusiones y recomendaciones preliminares

De acuerdo al análisis del caso se determina las siguientes conclusiones y recomendaciones preliminares:

- La evolución tecnológica ha generado la aparición de nuevo delitos.
- Las modalidades criminales de los delitos tradicionales se han combinado con los acontecimientos tecnológicos para generar una nueva clasificación de delitos.
- Uno de los problemas más grandes que enfrenta la justicia es la adaptabilidad de la tecnología a servidores públicos como jueces y fiscales.
- La evolución tecnológica ha propiciado que los delitos informáticos avancen, de manera que, ahora también se clasifican en delitos informáticos y computacionales.
- El desconocimiento parcial del tema por parte de los legisladores ha propiciado que al momento de redactar la norma existan vacíos legales, pues existen errores al formular el tipo penal, el verbo rector, y los sujetos del tipo penal.
- No existe una cultura digital efectiva capaz de informar sobre el avance legal y tecnológico a la sociedad, con la finalidad de evitar nuevas víctimas.
- Se necesita capacitar en estas nuevas modalidades delictivas a los entes judiciales.

- Es preciso determinar fiscalías especializadas en la materia dentro del Ecuador.
- Es indispensable el crear doctrina para entender la materia de mejor manera.
- Es necesario crear conciencia digital para evitar caer en este tipo de ilícitos

3. Criminología e Informática

3.1. Perfil criminal del atacante

3.1.1. Perfil del Delincuente Informático o Ciberdelincuente

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

Debemos partir del hecho que la palabra hacker es un término ampliamente generalizado, en el cual el común de la sociedad lo hace referencia o comparación a un pirata informático o delincuente, de allí el vocablo ciberdelincuente. Hay que considerar que dentro del Hacking hay una categorización de los sujetos que pertenecen a este fenómeno cibercriminal, así tenemos a los hackers, crackers, phreakers, viruckers, piratas informáticos, script kiddie, noob, newbie, lammer, dropper, carder, phisher, cyberstalker y otros; así mismo, una clasificación de los llamados hacker principalmente en: hacker negro (blackhat), hacker gris (greyhat), y hacker blanco (whitehat), términos recabados en el proceso de investigación y de acuerdo a Giménez (2011), descritos en los subtítulos posteriores.

3.1.2. Categorización de Sujetos en el Hacking

- *Hacker:* Es aquella persona que hace del hacking un arte, descubriendo y creando soluciones tecnológicas que puedan ayudar o beneficiar a un sector estratégico de la sociedad. Entre los más conocidos están Bill Gates (CEO de Microsoft), Mark Zuckerberg (Creador de Facebook), Jay Freeman alias Saurik (Creador de Cydia para dispositivos Apple).
- *Cracker:* Se dice de aquella persona dedicada a modificar, alterar o suprimir características esenciales de un programa o software con un fin malicioso o pecuniario. Los casos más comunes se dan en programas de paga, en los cuales el Cracker modifica el código del programa de paga para acceder a los beneficios totales del programa sin tener que pagar por la licencia de este. Entre los programas comúnmente crackeados están los antivirus y las versiones del sistema operativo Windows.

- *Phreaker:* Es la persona dedicada al hackeo de redes fijas y móviles. El pionero y más conocido Phreaker es John Draper alias Capitán Crunch[1], quien fue el primer hombre en hackear AT&T mediante un silbato.
- *Virucker:* Se dice que es la persona que se encarga del diseño, ensamblaje y creación a través de código malicioso de programas para transmitir o portar virus que infectan a los sistemas informáticos con el propósito de sustraer información o dañar sistemas. El más conocido es Robert Tappan Morris por crear el Gusano Morris en 1988, considerado como el primer gusano de ordenador de la era de Internet[2].
- *Pirata Informático:* Es aquella persona que, teniendo un conocimiento medio o avanzado de hacking, hace de esta una herramienta de trabajo para el cometimiento de actividades ilegales de tipo económico o financiero. En la actualidad hay cientos de piratas informáticos en todo el mundo, en las últimas dos décadas el más renombrado fue Vladimir Levin, quien fue acusado y preso por la Interpol después de meses de investigación por ser la mente maestra de una serie de fraudes tecnológicos que le permitieron a él y la banda que conformaba, substraer más de 10 millones de dólares, de cuentas corporativas del Citibank.
- *Script Kiddie:* Dícese de la persona que plagia y utiliza el código o script perteneciente a otra persona conocedora del hacking, con el fin de utilizar este código alardeando como si fuese de su autoría.
- *Noob o Newbie:* Dícese de la persona novata o principiante en el mundo de hacking, la cual busca adentrarse en esta temática con el fin de adquirir nuevos conocimientos en temas relacionados a la seguridad e inseguridad informática.
- *Lammer:* Dícese de la persona que se atribuye ser hacker sin poseer conocimientos de hacking.
- *Dropper:* Es la persona que se dedica a proveer y vender información concerniente a pines de seguridad y códigos CVV de tarjetas de crédito en todo el mundo. Normalmente en el mercado negro conocido también como Deep Web se encuentran proveedores o comerciantes que venden estos códigos de tarjetas de crédito. El precio entre comprar un código y pin para clonación de crédito oscila entre los 200 a 300 dólares americanos.
- *Carder:* Se dice que es la persona encargada de clonar tarjetas de crédito, en especial sus bandas magnéticas con un aparato electrónico llamado skimmer.

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

- *Phisher:* Es la persona que se dedica a clonar sitios web de diferente índole, con el fin de engañar al usuario final para la obtención de información de carácter sensible. Normalmente los llamados Phisher se dedican a la clonación de sitios web relacionados a la banca on-line para obtener datos que les permitan acceder a la cuenta del usuario para realizar transferencias bancarias.
- *Cyberstalker:* Dícese de la persona que hace uso del internet para acechar a su víctima sin ser detectado, abusando de la anonimidad que existente en el internet para cumplir con su fin. Vulgarmente se dice que el Cyberstalker es la persona que espía a otra a través del internet como en redes sociales con el fin de saber u obtener más información de esta sin que lo sospeche.

3.1.3. Clasificación de Hackers

- *Black Hat:* Los llamados Black Hat o hackers de sombrero negro, son aquellos que se encargan de violar la seguridad de sitios web, aplicaciones, base de datos y sistemas automatizados de información con propósito malicioso, a su vez buscan del hacking un peculio como forma de ganarse la vida.
- *White Hat:* Conocidos como hackers de sombrero blanco o Ethical hackers, se encargan de crear sistemas informáticos y programas con el propósito de beneficiar a un sector en específico de la colectividad, a su vez se encargan de explotar fallas y vulnerabilidades de sistemas informáticos con el fin de recomendar un lineamiento de protección en temas de seguridad de la información.
- *Gray Hat:* Un hacker de sombro gris, es aquel que se perfila entre un hacker negro y un hacker blanco, que ciertas veces actúa en el hacking de forma ética informando sobre vulnerabilidades y fallas en los sistemas, y otras veces explota estas de forma antiética para beneficio propio.

4. Ciberdelitos y derecho procesal penal

4.1. Nociones preliminares y avances en la materia en el Ecuador

El avance de la tecnología en la sociedad trae consigo una serie de aspectos, algunos que benefician y otros que perjudican, sobre los aspectos que perjudican, tenemos a los ciberdelitos, que si bien se encuentran normados bajo una ley sustantiva, en este caso el Código Orgánico Integral Penal, no están reglamentados bajo una base de acuerdos, resoluciones o guías interinstitucionales, si bien a decir de este investigador son varias las instituciones públicas que

"participan" o deberían participar en la investigación de estos delitos, otra es la realidad pre procesal y procesal penal.

Ahora bien, sobre el avance del Estado ecuatoriano en relación con los delitos cibernéticos, poco podemos decir, se evidencia un interactuar mínimo, partiendo del hecho que, a la actualidad solo contamos con una unidad de policía cibernética encargada de auxiliar a la fuerza pública y fiscalía en esta clase de delitos. El Ecuador aún no cuenta con fiscales ni jueces especializados en la materia, menos aun con una fiscalía especializada en tratar estos delitos, he ahí el resultado de tantos ciberdelitos que son archivados por falta de desconocimiento e impulso procesal.

4.2. Articulación de la Fiscalía General del Estado

4.2.1. Articulación con instituciones públicas para la persecución de los delitos informáticos

Antes de comenzar con este acápite, debo decir que me reservo el nombre de mis fuentes y de las personas entrevistadas, puesto que sus comentarios personales, no son los comentarios que representan al gobierno de turno, pudiendo crear este artículo académico a futuro, algún tipo de problema o consecuencia legal de los interactuantes de esta investigación. Además de que las falencias habladas con la mayoría de entrevistados corresponden a una realidad que el Estado por muchos años ha ocultado, y que sigue manteniendo en "secretismos" por no demostrar la ineptitud, inoperancia e ineficacia con la que funcionan a diario.

4.2.1.1. Ministerio del Interior

El Ministerio del Interior representa varias cuestiones, entre estas son los encargados de vigilar, custodiar y salvaguardar la seguridad ciudadana. Sobre este punto, la Policía Nacional como brazo ejecutor de esta cartera de estado y como ente auxiliar de la Fiscalía General del Estado, debido a lo señalado por el Código Orgánico de la Función Judicial, prevé no solo salvaguardar la integridad física de los ciudadanos, sino también la integridad digital.

Cuando hablamos de integridad digital, se nos viene a la mente muchas cosas, siendo los más certero el propugnar el respeto por la información, el dato, y la privacidad de cada uno de los hombres y mujeres de esta nación, en este sentido, existen departamentos y unidades de la Policía Nacional encargados de investigar, inteligenciar y colaborar para la persecución de los delitos cibernéticos que han menoscabado varios de los bienes jurídicos protegidos o tutelados por la Constitución de la República, leyes vigentes y convenios internacionales.

Para la presente investigación he solicitado información a varios entes y carteras de Estado, entre estos se ofició al Comandante General de la Policía Nacional con la finalidad de obtener información sobre lo que hacen varias de sus unidades y direcciones para la persecución de los delitos cibernéticos en colaboración con la FGE, de lo cual se obtuvieron los resultados que mencionaré en los siguientes acápites.

4.2.1.1.1. Dirección General de Inteligencia Policial

4.2.1.1.1.1. Unidad Nacional de Ciberinteligencia

Hubo la negativa de proveer la información que contiene esta unidad respecto a delitos cibernéticos, manifestando en oficio emitido por el Director General de Inteligencia Policial, textualmente lo siguiente: *Cabe informar que la Unidad Nacional de Ciberinteligencia si tiene coordinaciones de trabajo con la INTERPOL, dentro del ámbito de sus competencias por que maneja información específica la misma que se encuentra dentro de la clasificación de RESERVADO Y SECRETO de acuerdo a los establecido en el Art. 28 del Reglamento a la Ley de Seguridad Pública y del Estado (01 de Marzo del 2022).*

4.2.1.1.2. Dirección General de Investigación

4.2.1.1.2.1. Interpol Ecuador

Se organizó una reunión con el Jefe de la Interpol en el Ecuador, quien mencionó temas de relevancia para esta investigación, como la falta de articulación para trabajar de la mano con la Fiscalía General del Estado en casos de crimen organizado trasnacional sobre la investigación de delitos cibernéticos, indica además que no existe una articulación interinstitucional con otras instituciones para la persecución de delitos, menciona que Interpol Ecuador ha proveído de una base de datos para mejorar la búsqueda de estos delitos a la FGE.

Adicionalmente dice que las investigaciones en las que puede colaborar la Interpol con el estado ecuatoriano solo están direccionadas a la Dirección de Asuntos Internacionales de la Fiscalía y no al Ministerio del Interior, lo cual acarrea demoras, pues sin canales claros de comunicación para tramitar la información, solo resulta en pérdida tiempo para la investigación misma.

4.2.1.1.2.2. Unidad Nacional de Ciberdelitos

Aunque no se pudo concertar una reunión con el jefe de esta unidad por razones que desconozco, si puedo decir que se recibió parcialmente información solicitada mediante Oficio

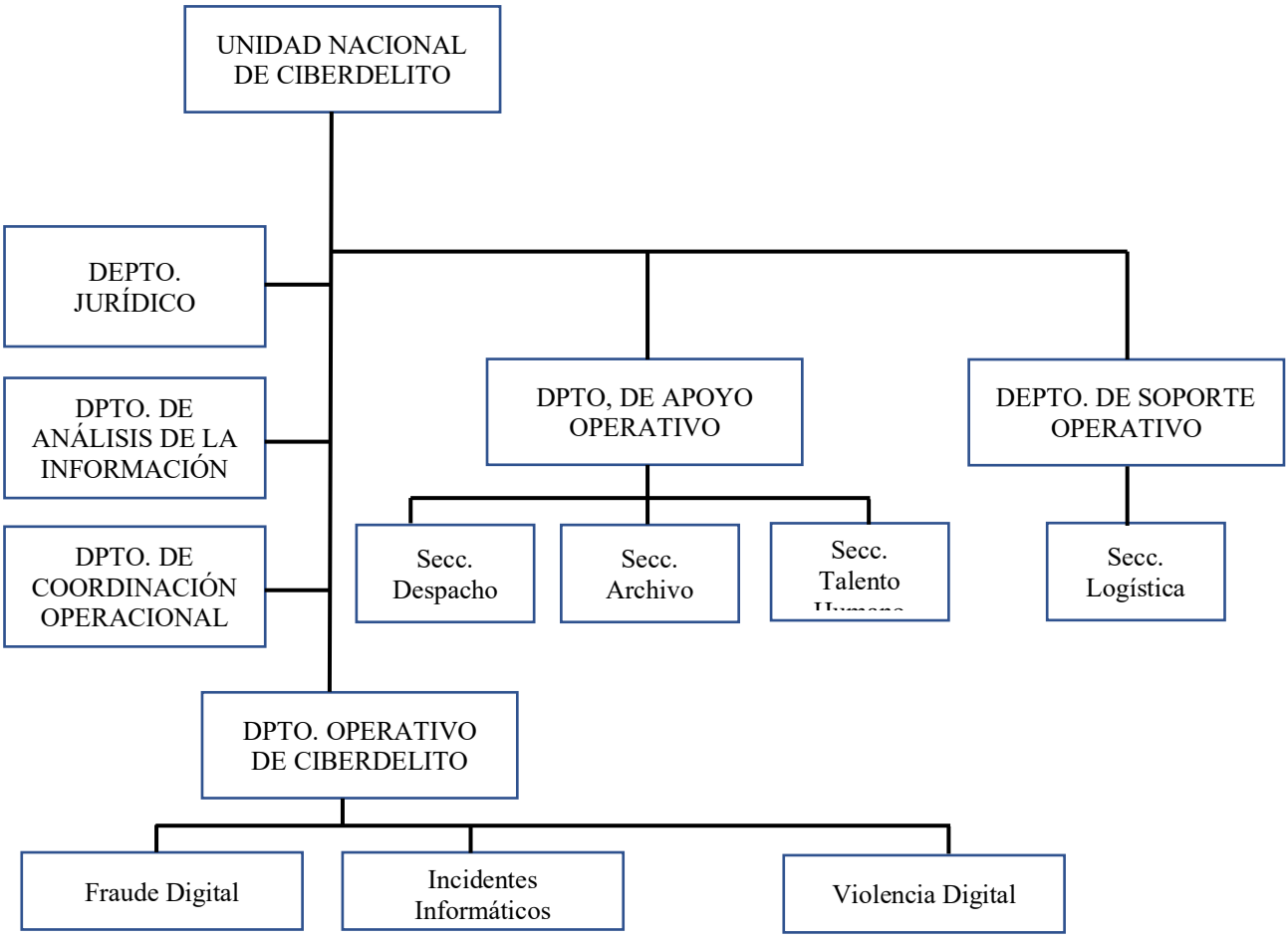
DIGIN-CIBERPOL-2022-0400-INF de fecha 10 de marzo del 2022, emitido por el sargento segundo de policía, Alfredo Salazar, asistente de talento humano de CIBERPOL (Unidad Nacional de Ciberdelitos), información que destaca lo siguiente:

Gráfico 1

Organigrama de la Unidad Nacional de Ciberdelito

Acuerdo Ministerial N.- 0080

De fecha 08 de marzo de 2019, suscrito por la Sra. Ministra del Interior, del "Estatuto Orgánico de Gestión Organizacional por Procesos de la Policía Nacional del Ecuador", consta la creación de la Unidad Nacional de Ciberdelito con el Departamento de Análisis de la Información según la siguiente figura:



Fuente: Unidad Nacional de Ciberdelito (2022)
Autor: Elaboración propia

En este cuadro se refleja el organigrama estructural de creación de la Unidad Nacional de Ciberdelito, mismo que inició en el año 2019, en el cual se destacan los departamentos:

- Departamento Jurídico
- Departamento de Análisis de Información
- Departamento de Apoyo Operativo
- Departamento de Soporte Operativo
- Departamento de Coordinación Operacional
- Departamento Operativo de Ciberdelito

Es importante conocer que todos estos departamentos reflejan las funciones de investigación del delito en esta materia, desde cuestiones administrativas, tales como solicitudes de fiscales y hacia fiscalía, así como el trabajo operativo de búsqueda de información en campo y en el ámbito digital.

Gráfico 2

Estadísticas delegaciones fiscales 2019-2021

Estadísticas de Delegaciones Fiscales investigadas por la Unidad Nacional de Ciberdelito, años: 2019-2020-2021

Se procedió a revisar las bases de datos de la Unidad, referente a las disposiciones fiscales recibida en materia de Ciberdelito, recibidas por año:

Fuente: Unidad Nacional de Ciberdelito (2022)
Autor: Elaboración propia

Los datos de este cuadro reflejan el número de delegaciones fiscales entre el año 2019 al 2021, en el que, según las estadísticas la cooperación entre la Fiscalía General del Estado y la Unidad Nacional de Ciberdelito, se llevó de la siguiente manera:

- Año 2019, un total de 828 delegaciones fiscales.
- Año 2020, un total de 632 delegaciones fiscales.
- Año 2021, un total de 1851 delegaciones fiscales.

De lo antes señalado, podemos notar claramente que entre el año 2019 y 2021, hubo un gran incremente del más del 100% en la perpetración de delitos cibernéticos. Adicionalmente, es importante conocer que existen un gran número de delitos investigados en cuya cooperación interviene por delegación fiscal la Unidad Nacional de Ciberdelito, la realidad procesal es que, la mayoría de estos delitos quedan en la impunidad, esto lo puedo comentar como ex servidor público de esta institución. Estadísticas o referencias sobre lo antes dicho, no serán encontradas, pues como conocemos, el Estado siempre procura denotar lo positivo y esconder lo negativo.

4.2.1.2. Centro de Inteligencia Estratégica

Me atrevería a decir que este es un Ministerio de adorno, puesto que, de las múltiples solicitudes realizadas, no se recibió ni siquiera la negativa. Si bien el Centro de Inteligencia Estratégica, antes llamado SENAIN es el máximo órgano de búsqueda y creación de inteligencia del Estado ecuatoriano, poco se sabe sobre su verdadero actuar, respecto al grado de involucramiento que tiene con la Fiscalía General del Estado, no se acerca en nada a beneficiar las investigaciones en diferentes delitos, sobre todo los informáticos.

4.2.1.3. Fuerzas Armadas

Se ofició al Comandante del Comando Conjunto de la Fuerza Armadas, como máxima autoridad de esta institución teniendo respuesta únicamente del Comando de Ciberdefensa.

4.2.1.3.1. Comando de Ciberdefensa

La respuesta recibida por el Comandante de Ciberdefensa del Comando Conjunto de la Fuerza Armadas, se circunscribió textualmente en lo siguiente: *"Al no contar con especialistas jurídicos militares en temas cibernéticos, es necesaria la colaboración de profesionales que puedan contribuir a la elaboración de una propuesta de Fuerzas Armadas, que sirva como insumo en las siguientes reuniones del Comité Interamericano contra el Terrorismo CICTE-*

OEA. Es preciso manifestar que los delitos informáticos se encuentran bajo responsabilidad de la Fiscalía y Policía Nacional; sin embargo, la detección de amenazas y riesgos a la infraestructura crítica digital de la defensa y del Estado por parte de actores al margen de la ley, es una responsabilidad compartida por todas las instituciones del Estado. Por lo expuesto, me permito recomendar a usted mi general de división, mantener una reunión para estudiar el alcance e intención de la solicitud del Dr. Alexander Cuenca Espinosa" (02 de marzo del 2022).

Podemos concluir de la mentada respuesta del COCIBER, que no cuentan con lineamientos o guías sobre la materia, menos con profesionales que conozcan bien de la rama, lo que hace notar que la cooperación institucional que pueda brindar esta comandancia a Fiscalía en pro de la persecución de los ciberdelitos es nula.

4.2.1.3.2. Comando de Inteligencia Militar Conjunto

No hubo respuesta del Comando de Inteligencia Militar sobre su colaboración con la Fiscalía para la persecución de ciberdelitos.

4.2.2. Articulación interdepartamental de la Fiscalía General del Estado

Si bien existen varios departamentos o direcciones de la Fiscalía encargados de brindar, transmitir e incorporar la información necesaria para la persecución de los delitos cibernéticos, la situación es otra, la actual Fiscal General del Estado desconoce de la realidad procesal penal de los ciberdelitos, partiendo del hecho que no tienen una Fiscalía especializada en la materia, que más allá del tema presupuestario, parte del hecho de una desorganización de cooperación interinstitucional, puesto que, la actual Fiscal General del Estado, no sabe el rol real que tiene cada una de las instituciones del Estado en beneficio de las investigaciones que deben realizarse.

Ahora bien, esta crítica no es de ahora, son estudios y vivencias que las he visto y compartido en mi lapso dentro del servicio público los últimos 10 años, al haber colaborado y trabajado con Fiscalía General del Estado, Ministerio del Interior y Secretaría del Inteligencia. Asombra que el mismo desconocimiento de hace 10 años atrás, lo siga tenido la Fiscalía a la actualidad, puesto que, no existe normativa, convenios o acuerdos interinstitucionales capaces de fortalecer la búsqueda de información para la persecución de los delitos materia de este trabajo académico, por otro lado, ese desconocimiento acarrea inoperancia que por consecuencia trae consigo impunidad frente al actuar de los ciberdelincuentes.

4.2.2.1. Actuaciones Fiscales

Las actuaciones fiscales relacionadas al tema de investigación se circunscriben a los actos urgentes emitidos por los Fiscales que tienen como principal motivo el conservar, precautelar y obtener la evidencia producto de los ciberdelitos, entre estas las que por extraterritorialidad y por temporalidad pueden permanecer un determinado tiempo, comúnmente esta evidencia digital es utilizada para armar la teoría del caso. Por otro lado, también pueden las actuaciones fiscales circunscribirse a los requerimientos que hacen a diferentes dependencias del Estado y del ente privado para descubrir la verdad de lo acontecido en un determinado caso, precautelando la información, intimidad y privacidad de los sujetos procesales –sospechosos y víctimas- mediante la correspondiente orden judicial para extraer, explotar, mantener, fijar y materializar las pruebas informáticas.

4.2.2.2. Coordinación General de Acceso a la Justicia

Se mantuvo una reunión con la actual autoridad de dicha coordinación, se hablaron de varias de las desventajas que presenta la Fiscalía en la persecución de los delitos informáticos, a decir de esta funcionaria de la Fiscalía General del Estado, existen los manuales y procedimientos, no solo establecidos por ley, sino también los internos de la institución, sin mencionar cuales son estos, además indico que estos no son públicos, todo lo antes dicho contraria a lo mencionado por autoridades de otras instituciones que en reuniones mencionan que no existe una articulación verdadera asentada en papeles con Fiscalía.

4.2.2.3. Dirección de Cooperación y Asuntos Internacionales

Una de las reuniones más fructíferas en lo que respecta a las autoridades en Fiscalía, en esta se trató temas importantes como la innovación de políticas y reglas internas que coadyuven a mejorar la administración de justicia en lo que respecta a la investigación pre procesal y procesal penal, en razón de esto la autoridad competente comentó que se encuentra en la creación de una Fiscalía especializada en ciberdelitos, la misma que constará de inicio con un Fiscal experto en la materia, sobre esto se dijo que la Fiscalía se estará especializando en la temática para brindar una atención más rápida, eficiente y oportuna a los requerimientos ciudadanos, por otro lado, se comentó acerca de los convenios que mantiene la FGE con otras instituciones en otros países, propugnando como siempre el respeto por la soberanía, sobre este punto de la ayuda internacional, se mencionó que el Ecuador es signatario de varios convenios, sin aun suscribirse el más importante en materia de cibercriminalidad que es el Convenio de Budapest, sobre este punto, mencionó que si bien existe la intención, el problema radica en las demoras de la

Cancillería, puesto que esta entidad al representar al estado ecuatoriano en el extranjero es la impulsora de la suscripción de los convenios de cooperación mutua.

4.2.2.4. Dirección de Investigación Civil

Si bien se ofició, y uno de los analistas de información de la Dirección de Investigación Civil se contactó con mi persona, hasta la fecha no se ha solventado las dudas planteadas, o se ha convocado a una reunión para tratar temas acerca de cómo está institución coopera en la búsqueda de información para el esclarecimiento de los delitos cibernéticos. Desde mi óptica como Ex Jefe Nacional del Departamento de Informática Forense y ex Investigador Civil de esta dirección, puedo mencionar que, dentro de esta se hacen los respectivos análisis e informes sobre casos de ciberdelitos, además se genera información e inteligencia útil para guiar a los fiscales dentro del proceso penal en la materia, por otro lado, a través de esta dirección los investigadores civiles tiene contacto con empresa como Microsoft o Facebook para obtener información conducente del delito investigado, tales como direcciones de correo, nombres, direcciones IP, fecha de creación de la información, etc.

4.2.2.5. Dirección de Estudios Penales

Se ofició y hubo respuesta de la señorita directora, quien de cierta manera indicó que su oficina nada tiene ver con los delitos cibernéticos, algo que desde mi humilde opinión es irrazonable por dos cuestiones: 1. La dirección de estudios penales debe encargarse del estudio penal y criminológico de estas nuevas modalidades delictuales para brindar más información y claridad a los fiscales de la materia, sobre todo en el cómo entender esta temática que cada vez toma más fuerza. 2. Los propios directores de otras áreas de la Fiscalía mencionaron que quien debe velar por un estudio penal de esta clase de delitos es la dirección de estudios penales. Concluyendo de esta manera que la autoridad no hizo más lavarse las manos sobre los requerimientos hechos, sin indicar una causa razonable.

4.2.2.6. Fiscalía Especializada en Delitos Cibernéticos y Telecomunicaciones FEDECI

Aunque en la actualidad no existe una fiscalía especializada en la materia, para el año 2017, presenté al Fiscal General del Estado encargado, Paúl Pérez Reina, una propuesta sobre la creación de una fiscalía que propugne las investigaciones esta clase de delitos, propuesta que incluía colaboración y cooperación internacional, en este caso por parte de la Fiscalía de Cibercrimen de la ciudad de Buenos Aires. Si bien dentro de la propuesta se incluía todo un

sistema, esto no involucraba inversión ni gasto presupuestario. Sin embargo, no se hizo nada, la razón clara, la falta de intención de la fiscalía para que se investiguen estos delitos.

4.2.3. Articulación de la Fiscalía General del Estado con entes privados

No existe a la actualidad convenios o acuerdos de cooperación entre la FGE y entes privados para la investigación de estos delitos, aunque debería existir acuerdo de peritos en la materia o laboratorio de informática forense.

5. Legislación y delitos cibernéticos

5.1. Ciberdelitos en la legislación ecuatoriana

Estos son algunos de los tipos penales más utilizados e importantes sobre ciberdelitos, cabe destacar que existen aún más de 30 tipos penales que puede adecuarse a conductas ilícitas cometidas o perpetradas a través o con la ayuda de la informática, las tecnología y telecomunicaciones en general y que se encuentran desde el COIP (2014).

Gráfico 3

Los Ciberdelitos en la Legislación ecuatoriana

Los Ciberdelitos	
C.O.I.P. Art. 174.	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos. – 7 a 10 años.
C.O.I.P. Art. 178.	Violación a la intimidad. – 1 a 3 años.
C.O.I.P. Art. 186.	Estafa. – 5 a 7 años
C.O.I.P. Art. 190.	Apropiación fraudulenta por medios electrónicos. – 1 a 3 años
C.O.I.P. Art. 191.	Reprogramación o modificación de información de equipos terminales móviles. – 1 a 3 años.
C.O.I.P. Art. 192.	Intercambio, comercialización o compra de información de equipos terminales móviles. – 1 a 3 años.
C.O.I.P. Art. 193.	Reemplazo de identificación de terminales móviles. – 1 a 3 años.
C.O.I.P. Art. 194.	Comercialización ilícita de terminales móviles. – 1 a 3 años.
C.O.I.P. Art. 195.	Infraestructura ilícita. – 1 a 3 años
C.O.I.P. Art. 229.	Revelación ilegal de base de datos. – 1 a 3 años.
C.O.I.P. Art. 230.	Interceptación ilegal de datos. – 3 a 5 años.
C.O.I.P. Art. 231.	Transferencia electrónica de activo patrimonial. – 3 a 5 años.
C.O.I.P. Art. 232.	Ataque a la integridad de sistemas informáticos. – 3 a 5 años.
C.O.I.P. Art. 233.	Delitos contra la información pública reservada legalmente. – 5 a 7 años.
C.O.I.P. Art. 234.	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. – 3 a 5 años.

Fuente: COIP (2014)
Autor: Elaboración propia

5.2. Situación actual de la persecución de los delitos cibernéticos en la región

La situación actual de los ciberdelitos apunta identificar que la mayoría de los países en Sudamérica goza de una legislación propia frente a esta clase de delitos, adicionando una fiscalía especializada en la materia, aquí es importante plantearnos: ¿Por qué siempre Ecuador está al último en las cuestiones legislativas e investigativas? ¿Es necesario reglamentar el actuar de la ley que castiga esta clase de delitos? Las respuestas a estas preguntas están sustentadas en el presente trabajo académico.

Gráfico 4

Convenios de Cooperación

Convenios de Cooperación suscritos	
▪ Tratado de Medellín	▪ Convención Interamericana sobre Asistencia Mutua en Materia Penal.
▪ Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional, Palermo 2000.	▪ Convención de las Naciones Unidas contra el Tráfico Ilícito de Estupefacientes y Sustancias Psicotrópicas
▪ Convención de las Naciones Unidas contra la Corrupción, Mérida 2003.	
Convenios de Cooperación NO suscritos	
Convenio de Budapest, aunque el Ecuador no es signatario de este convenio, es el más importante en materia de cibercriminalidad.	
¿Pero qué es el Convenio de Budapest? Es un acuerdo internacional para combatir el crimen organizado transnacional, específicamente los delitos informáticos, cuyo objetivo es establecer una legislación penal y procedimientos comunes entre sus Estados Partes. Está considerado como un referente obligado en los esfuerzos de la Comunidad Internacional para fortalecer el Estado de Derecho en el ciberespacio (Consejo de Europa sobre la Ciberdelincuencia, 2014).	

Fuente: COIP (2014)
Autor: Elaboración propia

6. Estadísticas actuales sobre ciberdelitos en el Ecuador

Estas estadísticas fueron obtenidas gracias a la Dirección de Asuntos Internacionales y la Dirección de Estadística de la Fiscalía General del Estado.

6.1. Estadísticas de ayuda mutua o cooperación penal internacional

Gráfico 5

Información de solicitudes de asistencia penal internacional en delitos cibernéticos 2018-2022

TIPO DE ASISTENCIA	AÑO	DELITO	INSTRUMENTO INTERNACIONAL Y PAÍS									
			CONVENCIÓN INTERAMERICANA SOBRE ASISTENCIA MUTUA EN MATERIA PENAL, NASSAU 1992			PRINCIPIO DE RECIPROCIDAD						
			EE. UU.	CÁNADA	PANAMÁ	RUSIA	NIGERIA	MALASIA	PAISES BAJOS	ALEMANIA	ESPAÑA	HONG KONG
PASIVA	2018	FRAUDE ELECTRÓNICO	1									
	2019	CONTRA LA INTIMIDAD Y CONTRA EL SECRETO DE LAS COMUNIDADES									1	
ACTIVA	2019	ACCESO NO CONSENTIDO A UN SISTEMA INFORMÁTICO, TELEMÁTICO O DE TELECOMUNICACIONES		1	1							
		APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS	2			1	1	1	1			
		ATAQUE A LA INTEGRIDAD DE SISTEMAS INFORMÁTICOS	1							1		
		DIFUSIÓN DE INFORMACIÓN DE CIRCULACIÓN RESTRINGIDA	2	1								
	2020	APROPIACIÓN FRAUDULENTA POR MEDIOS ELECTRÓNICOS	1									1
TOTAL			7	2	1	1	1	1	1	1	1	1
			17									

Fuente y elaboración: Dirección de Asuntos Penales y Cooperación Internacional FGE (2022)

La información contenida en este cuadro refleja el número de asistencias penales solicitadas por la Fiscalía General del Estado a otros entes en el exterior, algunos por convenios macro, y otros por principio de reciprocidad o asistencia mutua, de estos datos se destaca lo siguiente:

- Asistencias por convenio macro:
  - Año 2018: 1 asistencia
  - Año 2019: 8 asistencia
  - Año 2020: 1 asistencia
- Asistencias por principio de reciprocidad:
  - Año 2018: 1 asistencia
  - Año 2019: 5 asistencia
  - Año 2020: 1 asistencia

Dando un total de 17 asistencia penales entre el año 2018 y 2020.
De lo antes señalado, podemos denotar que el mayor número de asistencia penales fueron en el año 2019, así también, es importante conocer que, se podrían dar un mayor número de asistencias penales, si el Estado ecuatoriano fuera signatario del Convenio de Budapest también llamado Convenio de Cibercriminalidad.

6.2. Estadísticas nacionales

Gráfico 6

Información de solicitudes sobre noticias del delito 2019-2022

Fuente y elaboración: Dirección de Estadísticas y Sistema de la Información FGE (2022)

Gráfico 7

Información de solicitudes sobre noticias del delito 2019-2022

Provincia	Delito en tentativa o consumado	INTERCEPTACIÓN ILEGAL DE DATOS	OFERTA DE SERVICIOS SEXUALES CON MENORES DE DIECIOCHO AÑOS POR MEDIOS ELECTRÓNICOS	REEMPLAZO DE IDENTIFICACIÓN DE TERMINALES MÓVILES	REPROGRAMACIÓN O MODIFICACIÓN DE INFORMACIÓN DE EQUIPOS TERMINALES MÓVILES	REVELACIÓN ILEGAL DE BASE DE DATOS	TRANSFERENCIA ELECTRÓNICA DE ACTIVO PATRIMONIAL	ESTAFA		Total general
								Defraude mediante el uso de tarjeta de crédito, débito, pago o similares, cuando ella sea alterada, clonada, duplicada, hurtada, robada u obtenida sin legítimo	Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar,	
AZUAY	CONSUMADO	6	2	0	0	1	5	76	3	525
	TENTATIVA	0	0	0	0	0	0	0	0	4
	Total AZUAY	**6**	**2**	**0**	**0**	**1**	**5**	**76**	**3**	529
BOLIVAR	CONSUMADO	1	0	0	0	2	1	4	1	70
	Total BOLIVAR	**1**	**0**	**0**	**0**	**2**	**1**	**4**	**1**	70
CANAR	CONSUMADO	0	1	0	0	1	2	22	4	83
	TENTATIVA	0	0	0	0	0	0	0	1	2
	Total CANAR	**0**	**1**	**0**	**0**	**1**	**2**	**22**	**5**	85
CARCHI	CONSUMADO	0	1	0	0	1	17	6	0	186
	TENTATIVA	0	0	0	0	0	0	0	0	1
	Total CARCHI	**0**	**1**	**0**	**0**	**1**	**17**	**6**	**0**	187
CHIMBORAZO	CONSUMADO	2	0	0	0	5	3	49	6	255
	TENTATIVA	0	0	0	0	0	0	1	0	1
	Total CHIMBORAZO	**2**	**0**	**0**	**0**	**5**	**3**	**50**	**6**	256
COTOPAXI	CONSUMADO	2	0	0	0	1	6	87	4	291
	TENTATIVA	0	0	0	0	0	0	0	0	1
	Total COTOPAXI	**2**	**0**	**0**	**0**	**1**	**6**	**87**	**4**	292
EL ORO	CONSUMADO	9	2	0	1	3	8	31	5	537
	TENTATIVA	0	0	0	0	0	0	0	0	6
	Total EL ORO	**9**	**2**	**0**	**1**	**3**	**8**	**31**	**5**	543
ESMERALDAS	CONSUMADO	2	0	1	0	2	6	9	3	305
	TENTATIVA	0	0	0	0	0	0	1	0	5
	Total ESMERALDAS	**2**	**0**	**1**	**0**	**2**	**6**	**10**	**3**	310
GALAPAGOS	CONSUMADO	0	0	0	0	0	0	1	0	17
	TENTATIVA	0	0	0	0	1	0	0	0	1
	Total GALAPAGOS	**0**	**0**	**0**	**0**	**1**	**0**	**1**	**0**	18
GUAYAS	CONSUMADO	81	14	1	8	20	117	343	118	4.533
	TENTATIVA	1	0	0	0	1	2	7	1	106
	Total GUAYAS	**82**	**14**	**1**	**8**	**21**	**119**	**350**	**119**	4.639
IMBABURA	CONSUMADO	1	1	0	0	2	9	37	2	349
	TENTATIVA	0	0	0	0	0	0	0	0	3
	Total IMBABURA	**1**	**1**	**0**	**0**	**2**	**9**	**37**	**2**	352
LOJA	CONSUMADO	5	4	0	1	1	19	44	2	279
	TENTATIVA	0	1	0	0	0	0	0	0	4
	Total LOJA	**5**	**5**	**0**	**1**	**1**	**19**	**44**	**2**	283
LOS RIOS	CONSUMADO	5	1	1	0	2	36	156	17	506
	TENTATIVA	0	1	0	0	0	0	1	0	4
	Total LOS RIOS	**5**	**2**	**1**	**0**	**2**	**36**	**157**	**17**	510
MANABI	CONSUMADO	10	1	0	1	1	37	79	87	911
	TENTATIVA	1	0	0	0	1	0	0	0	11
	Total MANABI	**11**	**1**	**0**	**1**	**2**	**37**	**79**	**87**	922
MORONA SANTIAGO	CONSUMADO	0	0	0	1	0	0	12	1	88
	TENTATIVA	0	0	0	0	0	0	0	0	1
	Total MORONA SANTIAGO	**0**	**0**	**0**	**1**	**0**	**0**	**12**	**1**	89
NAPO	CONSUMADO	0	1	0	1	0	0	5	1	95
	TENTATIVA	0	0	0	0	0	0	0	0	2
	Total NAPO	**0**	**1**	**0**	**1**	**0**	**0**	5	1	97
ORELLANA	CONSUMADO	1	0	0	0	0	0	15	4	108
	TENTATIVA	1	0	0	0	0	0	0	0	2
	Total ORELLANA	**2**	**0**	**0**	**0**	**0**	**0**	**15**	**4**	110
PASTAZA	CONSUMADO	0	0	0	0	0	3	7	1	102
	TENTATIVA	0	0	0	0	0	0	0	0	1
	Total PASTAZA	**0**	**0**	**0**	**0**	**0**	**3**	**7**	**1**	103
PICHINCHA	CONSUMADO	85	6	0	1	45	58	1080	85	4.808
	TENTATIVA	2	0	0	0	0	0	12	2	49
	Total PICHINCHA	**87**	**6**	**0**	**1**	**45**	**58**	**1092**	**87**	4.857
SANTA ELENA	CONSUMADO	4	0	0	0	0	4	15	5	169
	TENTATIVA	0	0	0	0	0	0	1	0	4
	Total SANTA ELENA	**4**	**0**	**0**	**0**	**0**	**4**	**16**	**5**	173
SANTO DOMINGO DE LOS TSACHILAS	CONSUMADO	4	0	0	0	0	4	146	3	449
	TENTATIVA	0	0	0	0	0	1	1	0	2
	Total SANTO DOMINGO DE LOS TSACHIL	**4**	**0**	**0**	**0**	**0**	**5**	**147**	**3**	451
SUCUMBIOS	CONSUMADO	7	1	0	0	0	7	4	1	139
	TENTATIVA	0	0	0	0	0	0	0	0	1
	Total SUCUMBIOS	**7**	**1**	**0**	**0**	**0**	**7**	**4**	**1**	140
TUNGURAHUA	CONSUMADO	4	3	0	1	4	2	116	9	447
	TENTATIVA	0	0	0	0	0	0	1	0	1
	Total TUNGURAHUA	**4**	**3**	**0**	**1**	**4**	**2**	117	9	448
ZAMORA CHINCHIPE	CONSUMADO	1	0	0	0	1	7	**0**	**0**	26
	TENTATIVA	0	0	0	0	0	1	0	0	2
	Total ZAMORA CHINCHIPE	**1**	**0**	**0**	**0**	**1**	**8**	0	0	28
Total noticias del delito		**235**	**40**	**3**	**15**	**95**	**355**	**2.369**	**366**	**15.492**

	Total SANTO DOMINGO DE LOS TSACHIL	**9**	**265**	**7**	**0**	**11**	**0**	**0**	**0**	
SUCUMBIOS	CONSUMADO	12	96	1	0	9	1	0	0	
	TENTATIVA	0	1	0	0	0	0	0	0	
	Total SUCUMBIOS	**12**	**97**	**1**	**0**	**9**	**1**	**0**	**0**	
TUNGURAHUA	CONSUMADO	45	224	8	0	31	0	0	0	
	TENTATIVA	0	0	0	0	0	0	0	0	
	Total TUNGURAHUA	**45**	**224**	**8**	**0**	**31**	**0**	**0**	**0**	
ZAMORA CHINCHIPE	CONSUMADO	0	17	0	0	0	0	0	0	
	TENTATIVA	0	1	0	0	0	0	0	0	
	Total ZAMORA CHINCHIPE	**0**	**18**	**0**	**0**	**0**	**0**	**0**	**0**	
Total noticias del delito		**1.001**	**9.763**	**341**	**307**	**572**	**19**	**8**	**3**	

Fuente y elaboración: Dirección de Estadísticas y Sistema de la Información FGE (2022)

7. Conclusiones

El Estado ecuatoriano sigue siendo muy burocrático y secretista, no tiene el panorama claro para la persecución e investigación de los ciberdelitos, por parte de la Fiscalía General del Estado no existen las vías o canales adecuados para diligenciar una propia cooperación interinstitucional, pues las carencias de convenios, acuerdos, manuales o resoluciones internas derivan en que la mayoría de casos por delitos cibernéticos queden en el abandono e impunidad causando más agravios a las víctimas, adicionando que los casos investigados recaen en Fiscales inexpertos en la materia, lo cual conduce no solo a un deterioro de la fe que tiene la ciudadanía en la justicia, sino también en una demora propia de los entes estatales.

La ausencia de una fiscalía especializada en la materia trae consigo lentitud e inoperancia en las investigaciones, así también la ausencia de profesionales expertos en la temática. De acuerdo a las reuniones y entrevistas establecidas, el punto neurálgico del problema se desencadena porque la Fiscalía General del Estado como brazo ejecutor y titular de la acción penal, poco hace para prevenir estos delitos e investigarlos de la manera adecuada. Entendiendo que, sin una correcta directriz y sin nada asentado por escrito, nada se puede hacer sin los canales adecuados, todo se maneja de manera consuetudinaria, como bien creen y pueden.

Conforme a las estadísticas, se aprecia que los delitos de mayor consumación en los últimos 3 años son la estafa, el acceso no consentido a sistemas informáticos y la apropiación fraudulenta por medios electrónicos, sin menospreciar otras conductas delictivas que menoscaban los derechos de la ciudadanía. Es importante mencionar que los delitos cibernéticos como todo delito, centran su interés en el aspecto económico, sea afectando el peculio ajeno, como obtener información de interés que pueda ser vendida y resultar en beneficios ilegales, así como la afectación económica directa en modalidades cibercriminales como el banking o carding.

Es increíble como la impunidad crece día a día y los entes estatales como la Fiscalía General del Estado, hacen poco por ayudar a las víctimas de estas nuevas modalidades delictivas, si vemos la realidad, muchas de las veces incluso quienes reciben las denuncias en la entrada del órgano rector de la investigación penal, menciona que es mejor no hacer nada, porque a la final

poco se obtiene de los resultados sobre la investigación del crimen cometido, a esto sumarle la impunidad que se da en las cortes, cuando muchos de los jueces al encontrarse confundidos con estos nuevos tipos penales, lo que hacen es ratificar el estado de inocencia de los procesados.

Los desafíos de esta temática no solo destacan una investigación más ardua del tema, sino también acciones por parte del Estado para identificar los errores administrativos y judiciales que dejan estos delitos en la impunidad, considerando que el desafío más importante no es solo a nivel operación sino educacional.

Podemos finalizar comentando que, si bien en el Ecuador existe suficiente normativa penal para hacer punible estas conductas ilícitas, sin los mecanismos adecuados o las reglas del juego de quienes llevan a cabo la investigación penal, poco podremos hacer y seguiremos en un retraso no solo tecnológico, sino también jurídico.

Al concluir con el análisis de cada factor y ente jurídico en razón del cibercrimen en el Ecuador, queda en evidencia los vacíos estatutarios para la vigilia, sanción o pena que debe ejecutarse tras el cometimiento de un delito, y cuáles serían las bases jurídicas por las que las autoridades, funcionarios y entes reguladores deban actuar en razón de lo legal y en razón de la justicia, dejando en claro que los criminales y criminales están en todo lado, tanto en el ámbito digital como físico.

Gráfico 8

Caricatura de ciberdelitos

Fuente y elaboración: PC-PIXEL Tak (2012)

Este comic es un claro ejemplo que los criminales visten como cualquiera y que están en todo lado, gracias a la impunidad de justicia.

8. Recomendaciones

Si la Fiscalía General del Estado no se empapa del rol de cada una de las instituciones del Estado inmiscuidas en la investigación de ciberdelitos como protagonistas del eje pre procesal y procesal penal, nada se hará. Es necesaria no solo la creación de una Fiscalía especializada, sino también la creación de manuales, acuerdos, guías que reglamenten esta cooperación entre carteras de Estado, además de una constante actualización y preparación a Fiscales y Jueces, tarea que no solo depende de la FGE, también de la Escuela de Función Judicial perteneciente al Consejo de la Judicatura.

En conclusión, se recomienda:

- Generar lineamientos específicos para la articulación de la FGE con otras instituciones
- Generar manuales de procedimientos sobre la persecución de delitos cibernéticos
- Actualizar el conocimiento de los Fiscales dentro de la temática
- Crear la Fiscalía Especializada en Delitos Cibernéticos y Telecomunicaciones
- Cooperar a que el estado ecuatoriano sea signatario del Convenio de Budapest
- Elaborar las guías sobre prueba pericial informática con la ayuda de la Dirección de Investigación Civil y su laboratorio de informática forense
- Poner en funcionamiento el laboratorio de informática forense que le costó a la FGE algunos millones de dólares
- Crear acuerdo de cooperación con empresas privadas para la búsqueda de información relevante que ayude a esclarecer el delito informático investigado

9. Bibliografía, netgrafía, hemerografía y codificación en general

Bibliografía:

- Aboso, G. / Zapata, M. (2006). *Cibercriminalidad y Derecho Penal,* Buenos Aires, BdeF.
- Acurio, S. / Páez, J. (2010). *Derecho y nuevas tecnologías*, Quito, Corporación de Estudios y Publicaciones.
- Albrecht, H. / Sieber, U. (2009). *Criminalidad, evolución del derecho penal y crítica al derecho penal en la actualidad. Simposio Argentino – Alemán*, Buenos Aires, Editores del Puerto.

- Anzit Guerrero, R. (2011). *Derecho penal y paradigma criminológico en América Latina*, Buenos Aires, Cathedra Jurídica.
- Anzit Guerrero, R. / Tato, Nicolás. / Profumo, S. (2010). *El Derecho Informático. Aspectos Fundamentales*, Buenos Aires, Cathedra Jurídica.
- Anzit Guerrero, R. (2010). *Compendium criminis*, Buenos Aires, Lajouane.
- Astigueta, D. (2016). Reflexiones acerca de la naturaleza jurídica del proceso más breve. *Anuario Argentino de Derecho Canónico, 1 (22), 10 – 16.*
- Bazzell, M. (2013). *Personal Digital Security: Protecting Yourself from Online Crime*, CreateSpace Independent Publishing Platform, Estados Unidos.
- Berruezo, R. / Rodríguez, J. (2010). *Derecho penal económico*, Buenos Aires, BdeF.
- Bodmer, S. (2012). *Reverse Deception: Organized Cyber Threat Counter-Exploitation*, McGraw-Hill Education.
- Cabanellas, G. (2012). *Derecho de Internet,* Buenos Aires, Heliasta.
- Castro Arguello, M. (2009) / Tobares Catalá, G., *Delitos informáticos,* Buenos Aires, Advocatus.
- Cusa, G. (2013). *Criminalidad. El sujeto y su desafío a las normas*, Buenos Aires, Dunken.
- Fillia, L. / Monteleone, R. (2007). *Análisis integrado de la criminalidad informática*, Buenos Aires, Fabián Di Pladido.
- Granero, H. (2003). *El orden público tecnológico,* Buenos Aires, Educa.
- Hadnagy, C. (2011). *Ingeniería Social. El arte del hacking personal;* traducción de Montero, A., Madrid, Anaya.
- Ingenieros, J. (1913). *Criminología,* Madrid, Daniel Jorro.
- Jijena, R. (1992). *Chile. La protección penal de la intimidad y el delito informático*, Santiago, Jurídica de Chile.
- Kerr, O. (2016). *Computer Crime Law: 2016 Statutory and Case Supplement (American Casebook Series)*, Estados Unidos, West Academic Publishing.
- López, J. (2020). La pluralidad de víctimas derivadas de la elevada lesividad en los ciberdelitos: Una respuesta penal proporcional. *Estudios de Deusto, 1(68), pp. 201-218.*
- Lucero, P. / Kohen, A. (2010). *Delitos informáticos,* Buenos Aires, Ediciones D&D.
- Márquez, C. (2003). *El delito informático*, Bogotá, Leyer.
- Migliorisi, D. (2014). *Crímenes en la web,* Buenos Aires, Del Nuevo Extremo.
- Miró Linares, F. (2012). *El cibercrimen. Fenomenología y criminología de la delincuencia en el ciberespacio*, Madrid, Marcial Pons.

- Morillas, D. (2005). *Análisis dogmático y criminológico de los delitos de pornografía infantil,* Madrid, Dykinson.
- Muñoz Conde, F. (2007). *Introducción al derecho penal,* Montevideo, B de F.
- Palazzi, P. (2012). *Los delitos informáticos en el Código Penal. Análisis de la Ley 26.388*, Buenos Aires, Abeledo Perrot.
- Petrone, D. (2014) *Prueba Informática*, Buenos Aires, Ediciones Didot.
- Posada, R. (2017). El cibercrimen y sus efectos en la teoría de la tipicidad: de una realidad física a una realidad virtual. *Revista Nuevo Foro Penal. 13 (88), 71 – 112.*
- Poullet, Y. / Pérez Asinari, M. / Palazzi, P. (2009) *Derecho a la intimidad y a la protección de datos personales*, Buenos Aires, Heliasta.
- Riquert, M. (2009). *Delincuencia Informática. En Argentina y el Mercosur*, Buenos Aires, Ediar.
- Rivera, S. (2009). Los Delitos Informáticos. *Boletín Criminológico, 1 (1), 9 – 10.*
- Robideau, R. (2013). *Incognito Toolkit: Tools, Apps, and Creative Methods for Remaining Anonymous, Private, and Secure While Communicating, Publishing, Buying, and Researching Online*, Estados Unidos, Personal Armamento.
- Rodríguez, V. (2014). *Prueba y carga de la prueba en materia informática,* Buenos Aires, GOWA.
- Romero, C. (1987). *Poder informático y Seguridad jurídica,* Madrid, Editorial Fundesco.
- Sacoto, P. (2013). *Apuntes de Introducción al Derecho Penal,* Quito, PUCE.
- Sain, G. (2012). *Delito y nuevas tecnologías. Fraude, narcotráfico y lavado de dinero por internet*, Buenos Aires, Editores del Puerto.
- Singer, P. / Friedman, A. (2014). *Cybersecurity and cyberwar. What everyone needs to know*, Nueva York, Oxford University Press.
- Tarde, G. (2011). *Sociología criminal y derecho penal*; traducción de Blanco, A., Cabrera, D. y otros, Buenos Aires, AdHoc.
- Taylor, R. (2014). *Digital Crime and Digital Terrorism*, Estados Unidos, Prentice Hall.
- Telléz, J. (2006). *Derecho Informático*, México D.F, Mc Graw Hill.
- Tomeo, F. (2013). *Redes sociales y tecnologías 2.0*, Buenos Aires, Astrea.
- Touriño, A. (2014). *El derecho al olvido en internet*, Estado Unidos, Catarata.
- Ubiría, A. (2004). *Reparación de daños derivados del transporte benévolo*, Buenos Aires, Hammurabi.
- Vallejo, V. (2010). *Delito informático en la legislación ecuatoriana*, Quito, Corporación de Estudios y Publicaciones.

- Vaninetti, H. (2014). *Responsabilidad civil de los buscadores en internet,* La Plata, Editora Platense.

Netgrafía:

- Callegari, N. (2016). *Delitos Informáticos: Generalidades.* PUCE. Recuperado el 15 de marzo del 2022 de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
- Giménez, V. (2011). Hacking y Ciberdelito. Universidad Politécnica de Valencia. Recuperado el 15 de mayo del 2022 de https://riunet.upv.es/bitstream/handle/10251/11856/memoria.pdf
- González. M. (21 de diciembre 2004). El llamado ´Delito Informático´. Anales de la Facultad de Derecho, 21 (1), 45-65. Recuperado el 02 de febrero del 2022 de https://riull.ull.es/xmlui/bitstream/handle/915/18423/AFD_21_%282004%29_02.pdf?sequence=1.
- Levene, R. (02 de diciembre 2002). Introducción a los Delitos Informáticos, tipos y legislación. Recuperado el 20 de febrero del 2022 de http://www.delitosinformaticos.com/delitos/delitosinformaticos.shtml.
- Recovey labs. (01 de enero 2012), Definición de Delito Informático. Recuperado el 01 de marzo del 2022 de http://delitosinformaticos.info/delitos_informaticos/definicion.html.
- Sáenz, R. (01 enero 2013). Reforma del Código Penal Argentino. Recuperado el 20 el marzo del 2022 de http://delitosinformaticos.fiscalias.gob.ar/actualidad/reforma-del-codigo-penal/.
- SEGEN (01 de enero del 2020). *Delitos Cibernéticos – Nociones Básicas*. Recuperado el 15 de mayo del 2022 de https://www.casede.org/index.php/biblioteca-casede-2-0/seguridad/ciberseguridad/672-delitos-ciberneticos-nociones-basicas/file
- Viega, M. (01 de enero de 2011). *Un nuevo desafío jurídico: los Delitos Informáticos*. Departamento de Investigación UNAM. Recuperado el 15 de marzo del 2022 de http://mjv.viegasociados.com/wp-content/uploads/2011/05/DelitosInformaticos.pdf

Codificación, leyes y tratados en general:

- Constitución de la República de la Argentina.
- Constitución de la República del Ecuador.
- Código Penal argentino.
- Código Penal ecuatoriano.
- Ley 26.388 de la Argentina.
- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de datos del Ecuador.
- Convenio de Budapest sobre la Ciberdelincuencia.
- Registro Oficial., *Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Dato,* Quito, 2002. En: Suplemento Oficial No. 557.

Hemerografía

- Diario El Hoy., "Página web del Municipio de Quito destruida por crackers", en *Archivo Histórico,* Quito, 2001.
- Municipio de Quito., "Hackers destruyen página web del Municipio de Quito", en *Boletín de Prensa*, Quito, 2001.