UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA

FACULTAD DE JURISPRUDENCIA Y CIENCIAS POLÍTICAS

MAESTRÍA EN DERECHO

PROCESAL Y LITIGACIÓN ORAL

TEMA:

REGULACIÓN Y PROCESAMIENTO DE LOS CIBERDELITOS O DELITOS INFORMÁTICOS EN LA LEGISLACIÓN ECUATORIANA.

Trabajo de titulación, modalidad artículo profesional de alto nivel, previo a la obtención del título de Magíster en Derecho Procesal y Litigación Oral.

Autor(a)

Leslie Gabriela Pozo Caicedo

Tutor(a)

PhD. Marco Xavier Rodríguez Ruiz

QUITO – ECUADOR

2025

AUTORIZACIÓN POR PARTE DEL AUTOR PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TRABAJO DE TITULACIÓN

Yo, Leslie Gabriela Pozo Caicedo, declaro ser autora del Trabajo de Titulación con el nombre "Regulación y procesamiento de los ciberdelitos o delitos informáticos en la legislación ecuatoriana", como requisito para optar al grado de Magíster en Derecho Procesal y Litigación Oral y autorizo al Sistema de Bibliotecas de la Universidad Tecnológica Indoamérica, para que con fines netamente académicos divulgue esta obra a través del Repositorio Digital Institucional (RDI-UTI).

Los usuarios del RDI-UTI podrán consultar el contenido de este trabajo en las redes de información del país y del exterior, con las cuales la Universidad tenga convenios. La Universidad Tecnológica Indoamérica no se hace responsable por el plagio o copia del contenido parcial o total de este trabajo.

Del mismo modo, acepto que los derechos de autor, morales y patrimoniales, sobre esta obra, serán compartidos entre mi persona y la Universidad Tecnológica Indoamérica, y que no tramitaré la publicación de esta obra en ningún otro medio, sin autorización expresa de la misma. En caso de que exista el potencial de generación de beneficios económicos o patentes, producto de este trabajo, acepto que se deberán firmar convenios específicos adicionales, donde se acuerden los términos de adjudicación de dichos beneficios.

Para constancia de esta autorización, en la ciudad de Quito, a los 14 días del mes de marzo del 2025, firmo conforme:

Autor: Leslie Gabriela Pozo Caicedo Firma:
Firmado electrónicamente por:
LESLIE GABRIELA
POZO CAICEDO
Número de Cédula: 1004474902
Dirección: Imbabura, Ibarra, San Francisco Yacucalle
Correo electrónico: gabrielapozoab@hotmail.com
Teléfono: 0985330507

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación “Regulación y procesamiento de los ciberdelitos o delitos informáticos en la legislación ecuatoriana” presentado por Leslie Gabriela Pozo Caicedo, para optar por el Título Magíster en Derecho Procesal y Litigación Oral.

CERTIFICO

Que dicho trabajo de titulación ha sido revisado en todas sus partes y considero que reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del Tribunal Examinador que se designe.

Quito, 14 de marzo del 2025

MARCO XAVIER RODRIGUEZ RUIZ

Firmado digitalmente por MARCO XAVIER RODRIGUEZ RUIZ

……

PhD. Marco Xavier Rodríguez Ruiz
C.I.: 1710867597

DECLARACIÓN DE AUTENTICIDAD

Quien suscribe, declaro que los contenidos y los resultados obtenidos en el presente trabajo de titulación, como requerimiento previo para la obtención del Título de Magíster en Derecho Procesal y Litigación Oral, son absolutamente originales, auténticos, personales y de exclusiva responsabilidad legal y académica del autor.

Quito, 14 de marzo del 2025

.....

Leslie Gabriela Pozo Caicedo
C.I.: 1004474902

APROBACIÓN TRIBUNAL

El trabajo de titulación ha sido revisado, aprobado y autorizado su impresión y empastado, sobre el Tema: REGULACIÓN Y PROCESAMIENTO DE LOS CIBERDELITOS O DELITOS INFORMÁTICOS EN LA LEGISLACIÓN ECUATORIANA, previo a la obtención del Título de Magíster en Derecho Procesal y Litigación Oral, reúne los requisitos de fondo y forma para que el maestrante pueda presentarse a la sustentación del trabajo de titulación.

Quito, 14 de marzo del 2025

Firmado electrónicamente por:
ROMAN JOSE LUIS
TERAN SUAREZ

……..

Mg. José Luis Terán Suárez
PRESIDENTE DEL TRIBUNAL

Firmado electrónicamente por:
SANTIAGO DANIEL
MAYORGA ORTEGA

…….

Mg. Santiago Daniel Mayorga Ortega
EXAMINADOR

MARCO XAVIER RODRIGUEZ RUIZ

Firmado digitalmente por MARCO XAVIER RODRIGUEZ RUIZ

…….

PhD. Marco Xavier Rodríguez Ruiz
DIRECTOR

ÍNDICE DE CONTENIDOS

Tabla de contenido

TEMA..... i

AUTORIZACIÓN POR PARTE DEL AUTOR PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TRABAJO DE TITULACIÓN..... ii

APROBACIÓN DEL TUTOR..... iii

DECLARACIÓN DE AUTENTICIDAD..... iv

APROBACIÓN TRIBUNAL.....v

ÍNDICE DE CONTENIDOS vi

DEDICATORIA..... vii

AGRADECIMIENTO..... viii

RESUMEN ix

ABSTRACT x

INTRODUCCIÓN 1

DESARROLLO 2

Ciberdelitos o delitos informáticos 2

Invetigación de delitos informáticos 3

Prueba Digital..... 5

Normativa Jurídica. 6

Marco Normativo Internacional sobre ciberdelitos..... 6

Los ciberdelitos en la normativa vigente en el Ecuador..... 6

Análisis de caso No.2062-20-EP.....11

Caso: Ola Bini. 11

CONCLUSIONES. 12

REFERENCIAS BIBLIOGRÁFICAS 15

DEDICATORIA

Dedico este trabajo a mi familia, cuyo apoyo incondicional ha sido mi mayor fuerza ante este proceso académico. A mis padres quienes han sido ese pilar fundamental para forjarme en este camino con amor, perseverancia y ante todo con humildad. Y, a todos aquellos quienes me han acompañado en este camino personal y académico a quienes se los dedico con mucho cariño y mucho amor.

AGRADECIMIENTO

Expreso mi más sincero agradecimiento a mi tutor el PhD. Marco Xavier Rodríguez, quien con su sabio conocimiento me ha guiado y apoyado en el desarrollo de esta investigación. Agradezco a mis mentores y profesores, cuya guía ha sido invaluable en mi formación académica.

UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA

MAESTRÍA EN DERECHO PROCESAL Y LITIGACIÓN ORAL

TEMA: REGULACIÓN Y PROCESAMIENTO DE LOS CIBERDELITOS O DELITOS O DELITOS INFORMÁTICOS EN LA LEGISLACIÓN ECUATORIANA.

AUTOR: Leslie Gabriela Pozo Caicedo

TUTOR: PhD. Marco Xavier Rodríguez Ruiz

RESUMEN

La investigación se desarrolló sobre la situación normativa y jurídica de los delitos informáticos en el Ecuador, su tipificación, sanciones establecidas y el proceso para su investigación y juzgamiento, en perspectiva del avance de la tecnología y la suficiencia de la norma. Tema cuya importancia se encuentra en relación, no solo para su sanción, sino también con el entendimiento del manejo y protección de los datos y la información como derechos de las personas. En virtud de aquello la pregunta de la investigación es ¿Cuáles son las principales deficiencias del COIP en cuanto a la regulación y procesamiento de los ciberdelitos?, y como objetivo, plantear las principales deficiencias del COIP en cuanto a los ciberdelitos que ponen en riesgo distintos bienes jurídicos protegidos y sus posibles soluciones para salvaguardar el bienestar de estos. Dentro de los principales puntos de análisis se abordaron los siguientes ciberdelitos o delitos informáticos, prueba digital, normativa vigente y casos prácticos relacionados. Para ello, la metodología empleada tuvo un enfoque cualitativo, método hermenéutico jurídico, inductivo y deductivo, y técnicas como el análisis documental y de casos prácticos. Teniendo como resultados la postura del Ecuador frente a los delitos informáticos y lamentablemente se evidencian las necesidades y falencias para cubrir satisfactoriamente el juzgamiento y sanción de estos ilícitos ante una investigación carente de recursos, así como falta de capacitación y medios para cumplir con la seguridad jurídica y tutela judicial efectiva de los derechos y garantías frente a las conductas ilícitas en el ámbito tecnológico e información.

DESCRIPTORES: ciberdelitos, delitos informáticos, prueba digital.

UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA

FACULTY OF JURISPRUDENCE AND POLITICAL SCIENCE

Master's Degree in Procedural Law and Oral Litigation

AUTHOR: POZO CAICEDO LESLIE GABRIELA

TUTOR: PHD. RODRIGUEZ RUIZ MARCO XAVIER

ABSTRACT

REGULATION AND PROSECUTION OF CYBERCRIME OR COMPUTER CRIMES IN ECUADORIAN LAW

The research was conducted on the normative and legal situation of computer crimes in Ecuador, including their characterization, sanctions, and the process for their investigation and judgment, considering the advancement of technology and the adequacy of the standards. This issue is important, in relation not only to its punishment but also to understanding the handling, and protection of data and information as people's rights. Under that, the question of research is, what are the main shortcomings of COIP in regulating and prosecuting cybercrime? As a goal, it is necessary to raise the main shortcomings of COIP in terms of cyber-crimes that put at risk different protected legal assets and their possible solutions to safeguard the welfare of these. The main analysis included cybercrime, computer crimes, digital proof, current regulations, and related case studies. To achieve this, the methodology was built upon a qualitative approach, a legal, inductive, and deductive hermeneutic method, and techniques including documentary and case study analysis. Ecuador's position on computer crimes indicates the need and failure to cover properly the trial and punishment of these illegal acts, research resources and training are deficient. The technological and information fields lack the training and resources to comply with legal certainty, effective judicial protection of rights, and safeguards against unlawful conduct.

KEYWORDS:

Cybercrime, computer crimes, digital evidence

INTRODUCCIÓN

La tecnología ha avanzado de forma impresionante, tal es así que en la actualidad se tiene la automatización de la mayoría de los procesos industriales, científicos, mecánicos e incluso los mismos quehaceres domésticos, los aparatos y dispositivos electrónicos y tecnológicos han conquistado a la sociedad y es cada vez más común el manejo de esa tecnología y del internet en sus distintos dominios y redes sociales.

Al igual que el uso que se ha dado para el beneficio de la colectividad, y de las personas en forma individual, la tecnología ha sido empleada para cometer actos ilícitos, en especial el internet, espacio vasto en el que se ha ideado el cometimiento de una serie de delitos de toda clase, altamente perjudiciales para los ciudadanos.

En este contexto, se define como objetivo general: plantear las principales deficiencias del COIP en cuanto a los ciberdelitos que ponen en riesgo distintos bienes jurídicos protegidos y sus posibles soluciones para salvaguardar el bienestar de estos.

La presente investigación se desarrollará a fin de ampliar y determinar los principales indicadores respecto de la tipificación, juzgamiento y sanción de los delitos informáticos, así como la suficiencia del marco normativo y los recursos vigentes para su consecución, de esta manera, será posible identificar las debilidades y fortalezas que existen en este ámbito.

Será de gran utilidad para los estudiantes y profesionales del derecho como referente en la temática, y con atributos críticos en cuanto a la conveniencia y situaciones implícitas en cuanto a su aplicación en la práctica.

En el ámbito social será de utilidad del mismo modo para cualquier persona que se encuentre frente a una necesidad que involucre a esta clase de delitos, en lo académico es esta una herramienta teórico crítica referencial en cada uno de los componentes analizados, y en el ámbito jurídico cuenta con reflexiones profundas

de la normativa vigente, así como plantea necesidades y estrategias a ser atendidas para el debido procesamiento de estos ilícitos.

DESARROLLO

Ciberdelitos o delitos informáticos

Se ha avanzado tecnológicamente en el mismo sentido en cuanto al perfeccionamiento y amplitud del ámbito en el que se desarrollan los ilícitos, ahora en el espectro del internet a través de sitios y dominios web y el uso de redes sociales, existe un sinnúmero de ilícitos que se cometen con gran frecuencia y que van en aumento. Al respecto la fuente acota que los delitos informáticos son conductas ilícitas que se cometen a través del uso indebido de la tecnología vulnerando la privacidad de la información de terceras personas y empleándola para dañar o extraer aquellos datos que almacenan en gadgets o servidores, los cuales servirán para beneficio propio o de terceros (Acosta, Benavides & García, 2020).

Tal como se ha planteado es el mecanismo a través del cual se cometen estas conductas ilícitas lo cual lo define y lo hace particular, distinto del resto de ilícitos, e incluso como medio o mecanismo para el cometimiento de los delitos ordinarios tipificados con anterioridad a estos, por la naturaleza del internet y la complicidad te la confidencialidad de la identidad de quién está de cada lado de los ordenadores, ha hecho de estos ilícitos difíciles de investigar y sancionar.

Los delitos informáticos en estricto sentido desde los comportamientos que afectan al soporte de un sistema de tratamiento automatizado de almacenamiento de información que básicamente se compone de tres conductas ilícitas principales como lo son el espionaje el fraude y el sabotaje informático, sin que necesariamente se emplee para ello el Internet (Mayer & Calderón, 2020).

Cómo se había indicado con anterioridad es justamente el espacio en el que se desarrollan el que faculta gran variedad de estos delitos, la facilidad y simpleza para su cometimiento, y el alto nivel de dificultad para su persecución, juzgamiento y sanción, pese a los delitos enlistados con anterioridad, en la actualidad existe un

sin número de conductas ilícitas que se cometen a través del internet y el uso de la tecnología.

El cibercrimen o ciberdelincuencia es un fenómeno criminal que se ha potenciado en los últimos años dado el incremento y evolución de la tecnología y el uso democratizado de sistemas informáticos y redes sociales empleando el Internet en la sociedad, por lo que la tendencia indica que cada vez se invierte mayor tiempo del día en navegar en la Red por lo cual cada vez mayor información y datos personales se exponen al mundo virtual, por lo que en términos penales esto da entender que cada vez hay mayor información y datos personales en el ciberespacio lo cual facilita y aumenta la posibilidad de qué ciberdelincuentes dispongan de estos bienes jurídicos para su beneficio y vulneración (López, 2022).

Como se ha podido apreciar existen algunas posturas en cuanto a definir y caracterizar a los delitos informáticos o ciberdelitos, sin embargo, se puede concluir y concretar en que es el mecanismo de empleo de tecnologías o del internet el que define precisamente la existencia de un delito cometido en el ciberespacio, pudiendo tratarse incluso de delitos ya conocidos en los que se emplea este medio para llegar a su ejecución y alcanzar a su víctima.

Investigación de delitos informáticos

Como se ha indicado en líneas anteriores precisamente el mecanismo que se emplea para la ejecución y cometimiento de delitos informáticos o ciberdelitos es el que dificulta su investigación, ya que el internet es vasto y las herramientas imperceptibles.

El mejorar la detección del cibercrimen ha de considerar cada modalidad delincuencia en línea ya que cada una de ellas tiene su particularidad y la rentabilidad o el interés que presta para el infractor, por lo que, es importante analizar los distintos modus operandi y compartir este aprendizaje con los diferentes partes participantes del sistema de justicia penal (Toro, 2023, p. 169).

Sin embargo, en la actualidad se ha mejorado la seguridad en el internet, también conocida como ciberseguridad, al igual que se han difundido medidas a adoptar para una navegación segura, en efecto se ha conseguido pulir y mejorar el uso de redes sociales y dominios web, aun así, no ha sido posible combatir de forma drástica o eliminar el cometimiento de delitos informáticos.

Los ciberdelincuentes han desarrollado técnicas y habilidades para eludir medios y mecanismos de seguridad y poder perpetuar sus actividades ilícitas con el empleo de la tecnología y la oportunidad que presta también la exposición de información y datos personales en redes sociales, algunos de ellos tienen la capacidad de ocultar su identidad, huellas digitales ubicación e incluso correo electrónico y a la vez emplear los datos de sus víctimas para modificar rápidamente perfiles en línea lo cual les permite presentarse con múltiples identidades sin correr el riesgo de ser identificados y procesados (Curtis & Oxburgh, 2022).

Son muchos los mecanismos que se emplean para el cometimiento de delitos informáticos, y se suma a la complejidad de su investigación, lo imperceptible y camuflado de su actuar, puesto que no existen huellas o rastros evidentes o físicos que puedan ser recabados.

El modus operandi en la ciberdelincuencia se adecua a la metodología e intelecto de cada uno de los ciberdelincuentes así como la convicción que tienen para perpetrar el ilícito, medios que van desde correos falsos para aparentar representar entidades bancarias, links de páginas falsos, premios falsos, alertas de virus entre otros, los delitos de carácter informático emplean el fraude, el robo el engaño la extorsión y otros tipos de delitos ya registrados para perfeccionar y ejecutar su conducta (Saltos, Robalino & Pazmiño, 2021).

La misma tecnología e internet que han facultado el cometimiento de ilícitos, son los que se requieren para conseguir la investigación juzgamiento y sanción de los delitos informáticos, en el Ecuador se han implementado ciertas consideraciones, protocolos y procedimientos para la investigación de delitos

informáticos, sin embargo aún resta mucho por hacer y las herramientas e instrumentos son limitados para la implementación de la tecnología, capacitación y medios necesarios para conseguir un adecuada investigación y procesamiento de los ilícitos.

Prueba digital

Al tratarse de delitos cometidos a través del internet o de medios tecnológicos, no siempre se pueden conseguir pruebas físicas, evidencias documentales o materiales que puedan ser empleadas para la investigación y juzgamiento de los delitos informáticos.

La evidencia digital ha de cumplir con requisitos que verifiquen en realidad su autenticidad propios de su naturaleza, verificar además su fiabilidad integridad y disponibilidad, adicional a la licitud y legalidad para que en realidad sean valorados y respetados dentro de un proceso. La valoración de este tipo de evidencia se realiza en conjunto con el resto de actuaciones y medios probatorios del proceso, sumado a la sana crítica del juez, el mismo que ha de dar valor probatorio a medios electrónicos que puedan o tengan tendencia de ser modificados o manipulados por las partes o terceros (Gómez, 2020, p. 238).

En efecto existen indicios y evidencias que pueden ser recolectadas a través del uso de los mecanismos de investigación tecnológica y cibernética, como la identificación de direcciones, dispositivos o ubicaciones de los autores de los delitos informáticos, difíciles de recabar pero no imposibles, sin embargo, lo que se considera es su valoración en la administración de Justicia.

A partir de qué se expide la Ley de Comercio Electrónico que da apertura y libertad de admisión de mensajes de datos como mecanismos de prueba en los espacios judiciales, incluido al nuevo Código Orgánico General de Procesos, han existido varios avances doctrinarios y jurisprudenciales respecto al tratamiento y

participación que tienen estos estos mensajes de datos como material probatorio (Yepes, Pérez & Peinado, p. 272).

La prueba digital existe, la necesidad se lentifica en cuanto a la normativa aplicable para su procedencia, y el proceder adecuado para su valoración dentro de un proceso judicial, de tal forma que la prueba cumpla con su finalidad y respalde una postura, la tutela efectiva de derechos, sea en efecto verificable la existencia de un ilícito y la responsabilidad del participante.

Normativa jurídica

Marco normativo internacional sobre ciberdelitos

La normativa en el ámbito internacional ha sido fundamental para establecer mecanismos en cuanto al procesamiento y regulación de los delitos informáticos, pues los presentes convenios han buscado fortalecer este enemigo internacional. Por lo que, expongo los siguientes:

- Convenio de Budapest sobre la ciberdelincuencia, 2001
- Convenio de Berna sobre los derechos de autor, 2019
- La Convención para la Protección y Producción de Phonogramas de 1971 ratificado el 04 de junio de 1974.
- Convenio de París en 1993 sobre los derechos de autor con respecto a propiedad industrial.
- Convenio internacional de telecomunicaciones, suscrito en Nairobi -Kenya, el 6 de noviembre de 1982.

Los ciberdelitos en la normativa vigente en el Ecuador

El marco normativo en el Ecuador, respecto a los delitos informáticos, es mínimo, pero puntual y concordante en sus elementos, y ámbito de aplicación, es así que se tiene los siguientes cuerpos normativos, aplicables en la materia:

- Constitución de la República del Ecuador, 2008 (Ecuador).
- Código Orgánico Integral Penal, 2014 (Ecuador).

- Ley de Comercio Electrónico, Mensaje de Datos y Firmas Electrónicas, 2002 (Ecuador).
- Ley Orgánica de Protección de Datos Personales, 2021 (Ecuador).

El Código Orgánico Integral Penal, ha prescrito diversos artículos relacionados a delitos configurados mediante sistemas informáticos y dispositivos electrónicos, los cuales se detallan a continuación:

ARTICULO	**PRÁCTICA CIBERNÉTICA**	**BIEN JURIDICO**	**PENA**
Art. 103.- Pornografía con utilización de niñas, niños o adolescentes.	Fotografía, filmación, grabación, producción, transmisión o edición de materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico.	Integridad física y psicológica de los menores de edad.	13-16 años
Art.104.-Comercialización de pornografía con utilización de niñas, niños o adolescentes.	Publicite, compre, posea, porte, transmita, descargue, almacene, importe, exporte o venda, por cualquier medio.	Integridad y dignidad de los menores de edad	10-13 años
Art. 173.- Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos.	Contacto con un menor mediante algún medio electrónico o telemático con fines sexuales o eróticos.	Integridad sexual y reproductiva	1-3 años
Art. 174.- Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos.	Sexting.- Utilización de cualquier medio electrónico o telemático para ofrecer servicios sexuales.	Integridad sexual y reproductiva	7-10 años
Art. 178.- Violación a la intimidad.	Acceso y difusión de datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos.	Intimidad personal y familiar	1-3 años

Art. 182.- Calumnia.	La persona que, por cualquier medio, realice una falsa imputación de un delito en contra de otra.	Honor y buen nombre	6 meses – 2 años
Art. 185.- Extorsión.	Obtención de provecho personal mediante medios digitales, electrónicos para obtener un beneficio económico.	Propiedad	3 – 5 años
Art. 186.-Estafa.	Defraude mediante el uso de dispositivos electrónicos que alteren, modifiquen, clonen o dupliquen los dispositivos originales de un cajero automático para capturar, almacenar, copiar o reproducir información de tarjetas de crédito, débito, pago o similares (Carding)	Propiedad	5-7 años
Art.188.Aprovechamiento ilícito de servicios públicos.	La persona que altere los sistemas de control o aparatos contadores para aprovecharse de los servicios públicos (Robo de señal)	Propiedad	6 meses- 2 años
Art. 190.- Apropiación fraudulenta por medios electrónicos.	Utilización fraudulenta de un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno (Cracking)	Propiedad	1-3 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.	Propiedad	1-3 años
Art. 192.- Intercambio, comercialización o compra de información de equipos terminales móviles.	Intercambio, comercialización o compra de bases de datos.	Propiedad	1-3 años

Art. 193.- Reemplazo de identificación de terminales móviles.	Remplazo de etiquetas de fabricación de los terminales móviles.	Propiedad	1-3 años
Art.194.-Comercialización ilícita de terminales móviles.	Comercialización de terminales móviles con violación de la normativa de telecomunicaciones.	Propiedad	1 -3 años
Art. 195.- Infraestructura ilícita.	Posesión de programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de un equipo terminal móvil.	Propiedad	1 - 3 años
Art. 208A.- Actos lesivos a la propiedad intelectual.	Aquel que viole los derechos de propiedad intelectual con fines de lucro (Clonación de páginas)	Propiedad Intelectual	6 meses – 1 año
Art. 211.- Supresión, alteración o suposición de la identidad y estado civil.	Alteración de datos de identidad en programas informáticos, partidas, tarjetas índices, cédulas o en cualquier otro documento emitido por la Dirección General de Registro Civil.	Identidad	1 - 3 años
Art. 212.- Suplantación de identidad.	La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero. (Pishing)	Identidad	1-3 años
Art. 229.- Revelación ilegal de base de datos.	Revelación de 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. (SQL injection)	Seguridad de los activos de los sistemas de información y comunicación	1-3 años

Art. 230.- Interceptación ilegal de datos.	Interceptación de cualquier tipo de contenido mediante un sistema informático o dispositivo electrónico. (Sniffing)	Seguridad de los activos de los sistemas de información y comunicación	3-5 años
Art. 231.- Transferencia electrónica de activo patrimonial.	Manipulación de un sistema informático para procurarse la transferencia o apropiación no consentida de un activo patrimonial. (Cashout)	Seguridad de los activos de los sistemas de información y comunicación	3-5 años
Art. 232.- Ataque a la integridad de sistemas informáticos.	Obstaculizar de forma grave, deliberada e ilegítima el funcionamiento de un sistema informático. (Hacking)	Seguridad de los activos de los sistemas de información y comunicación	3-5 años
Art. 233.- Delitos contra la información pública reservada legalmente.	Utilización de información clasificada.	Seguridad de los activos de los sistemas de información y comunicación	5-7 años
Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	Acceso no autorizado a un sistema informático o de telecomunicaciones.	Seguridad de los activos de los sistemas de información y comunicación	3-5 años
Art. 298.- Defraudación tributaria, numerales 8,9 y 10.	Alteración a la administración tributaria mediante libros informáticos para evadir sus obligaciones.	Régimen de desarrollo	1-3 años

Fuente: Código Orgánico Integral Penal (2014)

Bajo estos convenios y normativas tanto nacionales como internacionales se refleja una iniciativa por parte del Ecuador para acoger parámetros que permitan regular los delitos informáticos en el país, así como lo ha realizado con el Convenio de Budapest acoplándolo a las normas prescritas en el COIP; sin embargo, los mismos han sido deficientes frente al ingenio que poseen los ciberdelincuentes para realizar sus ilícitos.

Conforme a la normativa vigente en el Ecuador, el sistema judicial ha enfrentado con herramientas limitadas una serie de procesos judiciales ligados a los delitos informáticos, que, dentro de la presente investigación han servido como directrices para estudiar el comportamiento y los resultados obtenidos en cuanto al procesamiento y regulación de los ciberdelitos.

Análisis de Caso No. 2062-20-EP

Carlos Alfredo Caiza Quillupangui presentó una denuncia en contra de Ramiro Miguel Baldeón Oñate el 05 de mayo del 2015, por el presunto delito de acceso sin consentimiento a un sistema informático, telemático o de comunicaciones (Art.234 del COIP). El 20 de noviembre del 2015 se realiza la audiencia de formulación de cargos, en donde se da inicio a la instrucción fiscal en contra de Ramiro Baldeón. Consecuentemente el 22 de febrero del 2018, se realiza la audiencia evaluatoria y preparatoria de juicio en la cual se resuelve dictar auto de llamamiento a juicio en contra del procesado. Con fecha 16 de julio el 2019 se realiza la audiencia de juicio en la cual el Tribunal ratifica el estado de inocencia de Ramiro Baldeón.

Se interpone recurso de apelación y posterior recurso de casación por Ramiro Baldeón con el fin de que la denuncia presentada en su contra se califique como maliciosa y temeraria más sin embargo la misma no es aceptada, llegando con su pretensión finalmente a la Corte Constitucional en el año 2021 mediante una acción extraordinaria de protección la cual no fue admitida a trámite.

Caso: Ola Bini

Ola Metodios Martin Bini fue detenido con fines investigativos el 12 de abril del 2019 en Ecuador por una presunta colaboración en la filtración de WikiLeaks, fundada por Julian Assange; con fecha 13 de abril se instala la audiencia de flagrancia en la cual Fiscalía pide prisión preventiva en contra de Bini misma que fue aceptada por el Juez de Garantías Penales. La defensa del procesado solicitó revocatoria y apelación a la prisión preventiva lo cual fue rechazado, sin embargo, frente a la acción de Habeas Corpus presentada a su favor un Tribunal de la Corte Provincial de Justicia de Pichincha concedió dicha acción y Bini recuperó su libertad.

Fiscalía acusó a Bini, en primer lugar, por el presunto delito de ataque a sistemas informáticos. Luego reformuló cargos por el ilícito de acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

El 03 de diciembre del 2020 se instala la audiencia evaluatoria y preparatoria de juicio en contra de Bini, en el cual la Juzgadora dicta auto de llamamiento a juicio en su contra por el delito acusado por parte de Fiscalía; consecuentemente el 19 de enero del 2022 se instala la audiencia de juicio la cual fue suspendida por varias ocasiones culminando el 31 de enero del 2023, luego de lo cual el Tribunal de juicio le ratifico su estado de inocencia lo cual quedo ejecutoriado.

De los casos descritos, se deduce que la prueba digital es uno de los muchos aspectos fundamentales a tener en consideración dentro del proceso judicial, mismas que son recabadas en una etapa pre-procesal y que tienen como finalidad verificar su autenticidad debiendo de aplicar una correcta cadena de custodia; Misma que, resulta ser ineficiente y carente de instrumentos y herramientas que la permitan actuar conforme al debido proceso.

CONCLUSIONES

La tipificación de los delitos informáticos en el COIP resulta insuficiente frente a los ataques cibernéticos y avance tecnológico que enfrenta el Ecuador y la

humanidad entera, por lo que se podría sugerir que es necesario que se reforme y se actualice con la misma fuerza en la que surgen los mecanismos para cometer los delitos informáticos, es decir a la par con la evolución y el desarrollo científico y tecnológico.

La principal herramienta para cometer el acto ilícito del que se integran los delitos informáticos es precisamente la web que afecta directamente a personas particulares o puede llegar inclusive al perjuicio del Estado, estos delitos se han incrementado en la actualidad por la facilidad que existe del acceso a la web por el cual se cometen, así como es atractiva la forma aparentemente imperceptible en la que el sujeto activo procede y del cual se desconoce la identidad y resulta casi imposible determinarla con facilidad, por lo que no sólo se ha magnificado el cometimiento de estos ilícitos sino que también se ha ampliado a nuevas formas de cometerlos y acceder a información y recursos privados de las personas a través de la red.

Con la investigación desarrollada, resulta necesario que el Estado ecuatoriano establezca suficientes políticas públicas sobre la criminalidad digital, que vayan direccionadas con la implementación de tecnología, la capacitación y recursos económicos para identificar y sancionar a los ciberdelincuentes.

Los esfuerzos por combatir los delitos informáticos y cibernéticos se vuelven limitados ante el abismal incremento de espacios para cometer los mismos, y la evolución a pasos agigantados que tiene la tecnología volviendo prácticamente inalcanzable la conjunción de medidas de seguridad y protección para estos sistemas y la persecución e investigación de las conductas ilícitas que puedan cometerse a través de este espectro. Por lo que se vuelve conveniente que se sume a toda medida de seguridad las que cada individuo debe observar y prever al compartir o acceder a ciertos sitios web y redes sociales para limitar de cierta forma el acceso a ciberdelincuentes, y proteger la información personal de la que pueden valerse para el cometimiento de ilícitos.

La normativa en el tema investigado que se encuentra vigente en el Ecuador presenta muchas falencias y limitaciones, de ahí que el COIP no cuenta con un apartado específico que determine un catálogo de delitos informáticos, sino más bien solo sanciona a ciertas actividades que atentan a la seguridad de la información, y la pena que estos establecen no va más allá de la privación de la libertad de tres a cinco años dependiendo el delito, y en ninguno de ellos se establece una sanción económica que repare la afectación hacia sus víctimas y consecuentemente hacia el Estado.

Es necesario que el Ejecutivo expida un reglamento como política criminal de Estado en el que se proteja la información del gobierno, las personas jurídicas y las personas naturales, en tanto que la tipificación de ciberdelitos que prevé el COIP con nuevos tipos penales, con las innovadoras estrategias que utilizan los hackers en el internet para obtener información de forma fraudulenta, porque siempre nos encontraremos vulnerables ya que existe el síndrome de estar conectados en la web, y utilización de dispositivos electrónicos.

Es imperativo que el gobierno determine nuevas fórmulas tecnológicas para la protección de la información que cada usuario posee considerando a esta como un bien que contiene una relevante importancia para sus actividades cotidianas. Así mismo, promueva a la ciudadanía mediante campañas, protocolos, seguros para que no estén vulnerables ante las diferentes amenazas que están presente en el internet.

El internet junto con otros adelantos de la tecnología ha hecho que la mayoría de actividades se conviertan en tareas más sencillas e incluso se prescinda por completo de la participación humana, los avances, sin embargo, también han facilitado el cometimiento de ilícitos, y han llegado a convertirlos en imperceptibles y difíciles de investigar, juzgar y sancionar. La norma se ve relegada ante los pasos agigantados de esta clase de ciberdelitos y su persecución demanda mejores y más instrumentos y herramientas de las que actualmente existen.

La insuficiencia de la norma se refleja en cuanto a la limitada tipificación de los ciberdelitos y su procesamiento, esto sumado a los recursos limitados destinados a la investigación y persecución de estos ilícitos. La tecnología que se requiere para investigar los ciberdelitos debe ser proporcional a los medios y mecanismos empleados para su cometimiento, y frente a ellos aún resta mucho por hacer para lograr una investigación y procesamiento satisfactorio.

Es necesario reformar el Código Orgánico Integral Penal, implementar instrumentos y un reglamento que establezca protocolos para la investigación de los ciberdelitos, tipificación y regulación adecuada de los ilícitos cometidos en esta modalidad, con penas proporcionales, sanciones económicas concretas y drásticas y personal capacitado en Fiscalía General del Estado para su investigación; normativa articulada y actualizada a la realidad es necesaria para que, se procese y sancione adecuadamente los ciberdelitos.

REFERENCIAS BIBLIOGRÁFICAS

ACOSTA, M., BENAVIDES, M. GARCÍA, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. Revista Venezolana de Gerencia

ACUARIO, S. (2016). Delitos Informáticos: Generalidades.

APARICIO, V. (2022). Delitos informáticos en Ecuador según el COIP: un análisis documental.

CARAGUAY, S. (2020). Aplicación de informática forense en auditorías gubernamentales para la determinación de indicios de responsabilidad penal con delitos informáticos en Ecuador, México y Perú, 2007- 2019

CARRERA, F., QUILLIGANA, J., AGUI- LAR, M., FIALLOS, S. (2019). Desafío de la ciberseguridad ante la legislación penal.

CURTIS, J., OXBURGH, G. (2022). Understanding cybercrime in ‘real world’policing and law enforcement. The Police Journal, 0(0), Ahead of Print. https://doi. org/10.1177/0032258X221107584

ENRÍQUEZ, J., ALVARADO, Y. (2015).

Los delitos informáticos y su penalización en el código orgánico integral penal ecuatoriano.

GÓMEZ, D. (2020). Implicaciones jurídicas de la evidencia digital en el proceso judicial colombiano. Ratio Juris: 220-240

JARA, L., FERRUZOLA, E., RODRÍGUEZ, G. (2017). Delitos a través redes sociales en el Ecuador: una aproximación a su estudio | I+D Tecnológico.

LÓPEZ, J. (2022). Sobre el alcance de los fines de la pena en el fenómeno criminal de la ciberdelincuencia. Revista Chilena de Derecho y Tecnología

MAYER, L., CALDERÓN, G. (2020). El delito de fraude informático: concepto y delimitación. Revista Chilena de Derecho y Tecnología

RODAS, P., LOOR, E. (2018). Proceso de formación en tipificación en el código orgánico integral penal para los delitos cibernéticos.

SACA, H., MARQUEZ, A., ARCINIEGAS, C. (2023) La Inviabilidad de la Prueba Digital por Falta de Regulación en los Delitos Informáticos.

SALTOS, ROBALINO, PAZMIÑO, (2021). Análisis conceptual del delito informático en Ecuador.

SÁNCHEZ, J., GONZÁLEZ, HIDALGO, C, ARCE, J., ORDÓÑEZ, P (2019). Análisis y revisión sobre delitos informáticos en el Ecuador.

SANTACRUZ, H., HERMOZA, M. (2019). Los delitos informáticos y su tipificación en la legislación penal ecuatoriana.

TORO, M. (2023). El control del cibercrimen. Análisis exploratorio de sentencias y medidas de supervisión. Revista Logos Ciencia & Tecnología: 162-173

YEPES, PÉREZ, PENADO, (2022). Aplicación de la prueba electrónica en el marco normativo colombiano. NovumJus: 253-277