593 Digital Publisher
CEIT
ISSN 2588-0705

Regulación y procesamiento de los ciberdelitos o delitos informáticos en la legislacion ecuatoriana

Regulation and processing of cybercrimes or computer crimes in Ecuadorian legislation

Leslie Gabriela Pozo-Caicedo [1]
Universidad Tecnológica Indoamérica - Ecuador
gabrielapozoab@hotmail.com

Marco Xavier Rodríguez-Ruiz [2]
Universidad Tecnológica Indoamérica - Ecuador
mrodriguez62@indoamerica.edu.ec

doi.org/10.33386/593dp.2025.1-1.3025

V10-N1-1 (ene) 2024, pp 193-204 | Recibido: 19 de noviembre del 2024 - Aceptado: 25 de enero del 2025 (2 ronda rev.)
Edición Especial

1 Maestranda del Programa de Posgrado en Derecho Procesal y Litigación Oral de la Universidad Indoamérica, sede Quito.
2 Docente del Programa de Posgrado en Derecho Procesal y Litigación Oral de la Universidad Indoamérica, sede Quito.

Cómo citar este artículo en norma APA:

Pozo-Caicedo, L., & Rodríguez Ruiz. M., (2025). Regulación y procesamiento de los ciberdelitos o delitos informáticos en la legislacion ecuatoriana. 593 Digital Publisher CEIT, 10(1-1), 193-204, https://doi.org/10.33386/593dp.2025.1-1.3025

Descargar para Mendeley y Zotero

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, nivel descriptivo, métodos 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.

Palabras claves: ciberdelitos, delitos informáticos, prueba digital.

ABSTRACT

The investigation was developed on the regulatory and legal situation of computer crimes in Ecuador, their classification, established sanctions and the process for their investigation and prosecution, in perspective of the advancement of technology and the sufficiency of the norm. A topic whose importance is related, not only to its sanction, but also to the understanding of the management and protection of data and information as people's rights. By virtue of this, the research question is: What are the main deficiencies of the COIP in terms of the regulation and processing of cybercrimes?, and as an objective, to raise the main deficiencies of the COIP in terms of cybercrimes that They put at risk different protected legal assets and their possible solutions to safeguard their well-being. Within the main points of analysis, the following cybercrimes or computer crimes, digital evidence, current regulations and related practical cases were addressed. To achieve this, the methodology used had a qualitative approach, descriptive level, legal hermeneutic, inductive and deductive methods, and techniques such as documentary analysis and practical cases. The results are Ecuador's position regarding computer crimes and, unfortunately, the needs and shortcomings are evident to satisfactorily cover the prosecution and punishment of these crimes in the face of an investigation lacking resources, as well as a lack of training and means to comply. with legal certainty and effective judicial protection of rights and guarantees against illicit conduct in the technological and information field.

Keywords: cybercrimes, computer crimes, digital evidence.

593 Digital Publisher CEIT ISSN 2588-0705

Introducción

Se define como pregunta de la investigación: ¿Cuáles son las principales deficiencias del COIP en cuanto a la regulación y procesamiento de los ciberdelitos?

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.

Método

Enfoque cualitativo

Se empleó el enfoque cualitativo considerando la naturaleza del fenómeno investigar, esto es los ciber delitos o delitos informáticos y su procesamiento en el Ecuador, a fin de priorizar los contenidos críticos, teóricos y jurídicos al respecto, contrastados que sean con el aporte del investigador y su juicio en torno al diagnóstico realizado y a las recomendaciones que sea posible plantear, se tiene también la técnica de campo de recolección de información de los protagonistas y conocedores en la materia, es así que se profundiza en el análisis del fenómeno desde su origen, proyectando sus efectos, y necesidades actuales.

Nivel descriptivo

Fue descriptivo considerando el enfoque documental que se le dio a la descripción y desarrollo de la presente investigación y la amplitud que se proyecta conseguir con el análisis de cada uno de los indicadores y puntos críticos que sean identificados en cuanto al procesamiento de los ciber delitos o delitos informáticos en el Ecuador, cuenta así el presente estudio con la contextualización y análisis de los fundamentos teóricos, y jurídicos vigentes al respecto, precedentes de investigaciones relacionadas y aportes críticos referenciales.

Métodos

Hermenéutico jurídico

Se empleó este método considerando la naturaleza de la figura de investigación, ya que fue necesario la revisión de las fuentes jurídicas y normativas que preceptúan lo referente a la

tipificación, investigación, procesamiento y sanción de los delitos informáticos o ciber delitos en el Ecuador, estas fuentes fueron analizadas y referidas de forma teórica y contrastadas con el pensamiento crítico del investigador seleccionado hacia el aporte novedoso de la presente.

Inductivo

En este ámbito se analiza el espectro de información con el que se cuenta tanto teórico como práctico a fin de identificar la existencia de una necesidad o problemática que en este caso ha sido identificada como la situación actual de la tipificación y procesamiento de los de ciber delitos o delitos informáticos en el Ecuador, esto conforme a los atributos y necesidades que han sido evidenciados de una revisión analítica y crítica de la normativa y la práctica en la administración de justicia.

Deductivo

Desde el ámbito deductivo fue posible partir desde la idea definida como problemática de la investigación en cuanto al procesamiento de los delitos informáticos ciberdelitos en el Ecuador, y desarrollar cada uno de sus elementos e indicadores a fin de ampliar y determinar sus causas, posibles efectos, y definir recomendaciones estratégicas tendientes a su solución.

Técnicas

Análisis documental: contrastando las fuentes teóricas, documentales, físicas y electrónicas referenciales en la materia y temática de investigación, de lo cual se determinaron aportes e indicadores puntuales a ser desarrollados en la discusión final con relación a los delitos cibernéticos en el Ecuador, y la normativa aplicable.

Análisis de caso: se tienen casos prácticos, como son pronunciamientos, fallos o sentencias que se han dado con relación a delitos informáticos en el Ecuador, donde se analizaron la aplicación y suficiencia de la normativa vigente en la materia, para el juzgamiento y sanción de estos.

Instrumentos

Ficha de análisis documental: graficando los principales hallazgos e indicios identificados de la aplicación de la técnica de análisis documental.

Ficha de análisis de caso: gráfico que recoge los principales aportes y conclusiones del análisis de casos en este estudio.

Resultados

Se consideran de forma preliminar las investigaciones y estudios realizados con anterioridad al presente, que han considerado o analizado uno o varios de los elementos que constituyen la problemática de investigación identificada en torno a la regulación y procesamiento de los ciberdelitos o delitos informáticos, y su aplicación localizada en el Ecuador, se tiene así:

En la investigación “Desafío de la ciberseguridad ante la legislación penal, sus autores Frank Alberto Carrera Calderón, Joel Estuardo Quilligana Barraquel, Mario Danilo Aguilar Martínez, Santiago Fernando Fiallos Bonilla (2019)”, destacan la importancia de este estudio en cuanto a explicar que en el Ecuador se tiene en la posición 55 de los países más vulnerables del mundo en cuanto a ciber delitos y los alcances de la legislación en virtud del caso de Julian Assange y su asilo político y ataques cibernéticos.

Se refiere en la mencionada investigación un punto crítico e indicador principal de la problemática objeto de la presente investigación, como lo es la ciberseguridad, ya que no solo plantea las medidas que podrían prevenir o identificar el cometimiento de ilícitos a través del ciberespacio, sino que además contribuye con la investigación y juzgamiento de esta clase de delitos.

En la investigación “Análisis y revisión sobre delitos informáticos en el Ecuador sus

Digital Publisher CEIT ISSN 2588-0705

autores Sánchez Jorge, González, Hidalgo Romero Cristian, Arce Rodríguez Juana, Ordoñez Barberán Plutarco (2019)", indican que la investigación se refiere al debido proceso en la normativa ecuatoriana respecto de los fraudes informáticos y delitos que tienen que ver con los sistemas de ordenadores para configurarlo.

El estudio contempla la consideración de estos delitos en el Ecuador, se circunscribe al debido proceso como una garantía básica de los derechos de protección considerados en la normativa constitucional vigente, definiendo su espectro en el estudio de los fraudes informáticos y aquellos delitos que son cometidos a través de la tecnología, estableciendo justamente la tipificación y consideración de los mismos en la normativa vigente.

En el estudio "Casos frecuentes, penalización y prevención de los delitos informáticos en el Ecuador: una breve revisión sistemática, Macías-Lara, Richard Alejandro, Boné Andrade, Miguel Fabricio, Quiñonez Angulo, Francisco, Mendoza Loor, José Javier, Estupiñan-Troya, Giuseppe, Rodríguez Vizuete, Jaime Darío (2022)", la investigación permitió conocer los métodos y alcances que utiliza los delincuentes para cometer ciber delitos y su postura en el sistema judicial ecuatoriano, considerando la reacción del Estado frente a los ataques informáticos en época de pandemia.

En esta investigación se plantea los casos frecuentes en cuanto a delitos informáticos y al tratamiento que la legislación vigente les da poniendo en evidencia la aplicabilidad y eficiencia que tiene la normativa vigente en la investigación, juzgamiento y sanción de estos ilícitos considerando precisamente un indicador principal de la finalidad que tiene el presente estudio, de identificar deficiencias existentes en la normativa penal aplicable.

En la investigación "Los delitos informáticos y su penalización en el Código Orgánico Integral Penal ecuatoriano, Enríquez Herrera Jhony Vicente, Alvarado Salinas Yasser César (2015)", señalan y se enfoca en el avance tecnológico en el Ecuador en los últimos años y en ese sentido el incremento que ha tenido la delincuencia que emplea el Internet, proyectando al respecto recomendaciones de procedimientos y posibles mejorías frente a ello.

Considera este estudio al Código Orgánico Integral Penal ecuatoriano y su investigación se basa justamente en el análisis histórico y cronológico de la aplicación de la normativa en cuanto a los delitos que han ido surgiendo con el tiempo y la evolución de la tecnología puntualizando el uso del internet y estableciendo recomendaciones y procedimientos que mejorarían el tratamiento de los mismos.

En el estudio "Los delitos informáticos y su tipificación en la legislación penal ecuatoriana, Hugo Santacruz, Magdalia Hermoza (2019)", estudia la posición jurídico penal de la normativa vigente en el Ecuador en relación a los ciber delitos además de considerar aspectos y puntos críticos respecto de una mejora en la administración de justicia.

Este estudio puntualiza en la forma en la que han sido tipificados los delitos informáticos en el Ecuador y su contraste con las normas aplicables en este caso se establece un análisis jurídico y crítico en cuanto a los ciber delitos a través de la normativa vigente y se puntualizan consideraciones prioritarias de recomendaciones que mejorarían la administración de Justicia en estos casos.

En el trabajo titulado "Proceso de formación en tipificación en el Código Orgánico Integral Penal para los delitos cibernéticos Rodas Soto Patricia, Loor Elizabeth (2018)", concluyen y abordan los ilícitos informáticos que son tipificados y considerados en la legislación ecuatoriana determinando la problemática en cuanto a la configuración como delitos en consonancia con el avance de la tecnología.

En la antes mencionada investigación se consideran a los delitos informáticos y su penalización dentro de la normativa ecuatoriana como un problema que causa la confusión o la falta de determinación adecuada de la configuración de estos ilícitos a fin de identificarlos como tal

y atribuirles una sanción proporcional dentro del debido proceso y culminar con el juzgamiento satisfactorio de estas conductas.

En la investigación "Retos de la administración de justicia penal frente a los delitos informáticos en el ecuador, Hernández Katherine (2016)", se refiere a los retos que ha tenido la administración de justicia para alcanzar una investigación y sanción de los delitos informáticos adicional al reto que tienen las instituciones para investigar estos ilícitos en el Ecuador.

Esta investigación es importante en cuanto al aporte que tiene al plantear la identificación de los retos que tiene la administración de Justicia para el adecuado procesamiento de los delitos informáticos, que es precisamente uno de los elementos que constituyen la problemática de la presente investigación y que sin embargo, es particular su aporte en cuanto a los retos que han sido identificados en las instituciones que están encargadas de investigar estos delitos, planteando recomendaciones estratégicas de atención.

En la investigación "La Inviabilidad de la Prueba Digital por Falta de Regulación en los Delitos Informáticos, Saca Condo Henry, Marquez Barreto Anthony, Arciniegas Castro Cesar (2023)", refiere la creación de nuevos instrumentos para medios de prueba digital ya que los medios tradicionales de prueba documentales periciales y testimoniales no abastecen los requerimientos y el alcance que demanda las investigaciones de nuevos delitos.

En el mencionado estudio se refiere otro de los indicios y elementos de la problemática de la presente investigación en cuanto a la prueba digital considerada como inviable dentro de lo que se ha determinado como regulación de los delitos informáticos, e identifica precisamente la necesidad de que se creen nuevos instrumentos para tratar este tipo de medios probatorios indispensables en la investigación y juzgamiento de esta clase de delitos.

En el estudio "Delitos a través redes sociales en el Ecuador: una aproximación a su estudio I+D Tecnológico, Jara Luis, Ferruzola Enrique, Rodríguez Guillermo (2017)", se refiere al comportamiento jurídico y su alcance en referencia a la normativa ecuatoriana sobre los delitos cibernéticos enfocándose principalmente en aquellos que utilizan a las redes sociales para acercarse y cometer las conductas delincuenciales con usuarios de estas plataformas.

Tratando el caso especial del cometimiento de delitos a través de las redes sociales en el Ecuador este estudio analiza la suficiencia de la normativa vigente en cuanto al tratamiento de los delitos cibernéticos en este país considerando el caso especial de la red social Facebook y la facilidad que tienen los delincuentes para acercarse a sus víctimas a través de este tipo de redes sociales.

En el trabajo titulado "Delitos informáticos en Ecuador según el COIP: un análisis documental, Aparicio Izurieta Viviana Vanessa (2022)", se refiere al compendio de modos y fines que tienen los delincuentes a través del uso de la tecnología para cometer delitos de carácter cibernético informático y plantear una posible solución en cuanto a la posición del Estado para respaldar y garantizar la seguridad y confidencialidad de la información de los ciudadanos.

En esta investigación se tiene como aporte el análisis documental en cuanto a la modalidad y finalidad que se persigue en cada uno de los delitos informáticos y la perspectiva que tienen los delincuentes en cuanto a la intencionalidad con la que se cometen, identificando las necesidades y recomendaciones en cuanto al mantenimiento de la seguridad de la información en la web y la confidencialidad informática, como mecanismos no solo de prevención sino también de reparación ante delitos de esta naturaleza.

En la investigación "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, Caraguay Ramírez Stalin Xavier (2020)", aborda la posibilidad de implementar una rama

593 Digital Publisher CEIT ISSN 2588-0705

de las ciencias forense con enfoque informático dentro del sistema judicial y de investigación como una herramienta que contribuya en la indagación y correcta definición de responsabilidad respecto de los delitos informáticos.

La ciencia forense es imprescindible en cuanto a la investigación de los delitos, más aún en este caso cuando se trata de delitos aparentemente imperceptibles, y que se dificulta su persecución e identificación, por lo que se aporta con la recomendación de implementar un sistema de informática forense dentro del sistema de administración de justicia como una herramienta eficaz en la investigación y sanción adecuada de los delitos informáticos.

En el trabajo "Delitos Informáticos: Generalidades, Acuario del Pino Santiago (2016)", se enfoca en el retroceso que el derecho penal ha tenido frente a los delitos nuevos, definiendo la necesidad de reformar la normativa penal vigente para que se amplíe y contemple nuevas conductas ilícitas y se configuren en ese sentido delitos y sanciones proporcionales atribuidas a los responsables de delitos informáticos, en garantía del derecho a la seguridad jurídica reconocido por el Estado.

Como se ha podido evidenciar existen algunos estudios e investigaciones que se han desarrollado en torno a uno o varios de los elementos que constituyen la problemática identificada para la presente investigación, esto es, en cuanto a la tipificación, juzgamiento y sanción de los delitos informáticos o ciber delitos en el Ecuador, sin embargo, la presente investigación es original y novedosa en el sentido de cubrir la necesidad de aportar con una investigación analítica y crítica en cuanto a las deficiencias que se puede evidenciar del vigente Código Orgánico Integral Penal en lo de delitos, por lo que se plantea el desarrollo de un estudio consolidado respecto de cada uno de los elementos que integran esta problemática.

Contexto conceptual

Ciberdelitos o delitos informáticos

Con el avance de la tecnología se ha avanzado 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 ciber crimen o ciber delincuencia ere un fenómeno criminal que sea potenciado en los últimos años dado el incremento y evolución de la tecnología y el uso de 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 ciber espacio lo cual facilita y aumenta la posibilidad de qué ciber delincuentes dispongan de estos bienes jurídicos para su beneficio y vulneración (López, 2022).

Como se ha podido apreciar existen algunas posturas en cuanto a de definir y caracterizar a los delitos informáticos o ciber delitos, 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 ciber crimen 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 ciber delincuentes 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 modo operandi en la ciber delincuencia se adecua a la metodología e intelecto de cada uno de los delincuentes así como la convicción que tiene 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 el caso de investigación de delitos informáticos, sin embargo aún resta mucho por hacer y los recursos son limitados para la implementación de la tecnología, capacitación y medios necesarios para conseguir un adecuado 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 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 concibe principalmente los siguientes instrumentos:

✓ 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:

✓ Código Orgánico Integral Penal, 2014 (Ecuador).

✓ Constitución de la Republica del Ecuador, 2008 (Ecuador).

✓ Ley de Comercio Electrónico, Mensaje de Datos y Firmas Electrónicas, 2002 (Ecuador).

Análisis de Caso

Caso No. 2062-20-EP

Carlos Alfredo Caiza Quillupangui presentó una denuncia en el año 2015 en contra de Ramiro Miguel Baldeón Oñate por el supuesto delito de acceso sin consentimiento a un sistema informático, telemático o de comunicaciones. Posteriormente se realiza la audiencia de formulación de cargos en donde se decide acoger el pedido de fiscalía y se da inicio la instrucción fiscal en contra del denunciado. Tras lo cual se desarrolla la audiencia devaluatoria y preparatoria de juicio en la que se resuelve dictar auto de llamamiento a juicio en contra del antes indicado denunciado y otros precisamente por la presunta participación el ya indicado delito tipificado en el artículo 234 del COIP.

Finalmente, el Tribunal de Garantías Penales realiza la audiencia de juicio y resuelve ratificar el estado de inocencia del procesado y se cancelan las medidas cautelares dictadas previamente. Se impugna esta decisión y se interpone recurso de apelación por parte del proceso pesado el cual solicitaba que se declare la denuncia como maliciosa y temeraria, en esta audiencia de apelación se resolvió ratificar la inocencia y la sentencia subida en grado, negando así lo solicitado por el accionante al determinar que no existió ni malicia ni temeridad en la acusación particular. A lo cual se interpone recurso de casación el cual fue inadmitido por los jueces correspondientes, resultando finalmente en la decisión del accionante de interponer acción extraordinaria de protección.

Caso: Ola Bini

Bini fue detenido en el año 2019 en Ecuador mientras se disponía a viajar a Japón, esto a la par de la finalización del asilo que beneficiaba a Julian Assange en su embajada en Londres. Se procede a la detención del australiano quién era considerado el fundador de WikiLeaks en Reino Unido, también requerido por el gobierno de Estados Unidos para que sea extraditado por los cargos de filtración de información reservada que expuso al gobierno de Washington.

La fiscalía ecuatoriana acusó a Bini por la sospecha de que el procesado había ingresado sin autorización al sistema de la Corporación Nacional de Telecomunicaciones (CNT). En el proceso se resolvió finalmente en el año 2022 desistir de seguir el proceso a lo cual fiscalía apeló. Luego de que se analicen los elementos se resolvió que no fue posible probar las teorías sobre el acceso sin consentimiento a un sistema telemático, así como la falta de pertinencia de las pruebas y argumentos probatorios presentados, por lo que se resolvió ratificar el estado de inocencia del acusado.

Discusión

La normativa que se encuentra vigente en Ecuador para regular los delitos informáticos es bastante sencilla y se aplica de forma generalizada sin mayor especificidad en cuanto a la distinción de los ilícitos y su investigación, por lo que se podría sugerir que es necesario que se reforme acorde al principio de progresividad y se actualice de la misma forma en la que los mecanismos para cometer los delitos informáticos lo hacen, es decir a la par con la evolución y el desarrollo científico y tecnológico.

El principal recurso para cometer el acto ilícito del que se integran los delitos informáticos es precisamente la web qué afecta directamente a personas particulares o puede llegar al perjuicio del estado, estos delitos se ven en incremento día con día por la facilidad que existe del acceso al recurso por el cual se cometen, así como es atractiva la forma aparentemente imperceptible en la que el actor procede y del cual se desconoce la identidad y resulta casi imposible determinar la con facilidad, por la 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.

593 Digital Publisher CEIT ISSN 2588-0705

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 delincuentes cibernéticos, y proteger la información personal de la que pueden valerse para el cometimiento de ilícitos.

Las leyes que se encuentran vigentes en el Ecuador presentan muchas falencias, el COIP no cuenta con un apartado dedicado a los delitos informáticos, solo sancionan a ciertas activades 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, y en ninguno de ellos se establece una sanción económica ante el cometimiento de este tipo de contravenciones.

Es necesario que estructuren o planteen nuevas leyes para proteger la información de los gobiernos, empresas y las personas, pero con los avances tecnológicos que surgen cada día y las nuevas estrategias que utilizan los hackers en el internet para obtener información de forma fraudulenta siempre nos encontraremos vulnerables ya que nos vemos en la necesidad de estar conectados en la web.

Es imperativo que el gobierno determine nuevas fórmulas de 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.

Conclusiones

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 recursos de los que actualmente existen.

La insuficiencia de la norma se refleja en cuanto a la limitada definición y 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 normativa nueva que establezca protocolos para la investigación de los ciberdelitos, tipificación y regulación adecuada de los ilícitos cometidos en esta modalidad, con penas proporcionales y personal capacitado para su investigación y juzgamiento. Normativa articulada y actualizada a la realidad es necesaria para que, conforme al principio de progresividad 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., AGUILAR, 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. Conrado

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