ESCUELA DE JURISPRUDENCIA

Tema:

JURISDICCIÓN UNIVERSAL EN CIBERDELITOS EN LA LEGISLACIÓN ECUATORIANA

Proyecto de investigación previo a la obtención del título de Abogada

Línea de investigación:

DERECHO, PARTICIPACIÓN, GOBERNANZA, REGÍMENES POLÍTICOS E INSTITUCIONALIDAD

Autora:

Camila Salomé Paredes Robalino

Director:

Mg. Christian Danilo Gavilanes Domínguez

Ambato – Ecuador

Febrero 2025

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **CAMILA SALOMÉ PAREDES ROBALINO,** con cédula de ciudadanía **1850180389,** autora del trabajo de graduación titulado: "JURISDICCIÓN UNIVERSAL EN CIBERDELITOS EN LA LEGISLACIÓN ECUATORIANA", previa a la obtención del título profesional de **ABOGADA,** en la escuela de **JURISPRUDENCIA.**

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, febrero 2025

Camila Salomé Paredes Robalino

CC. 1850180389

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

JURISDICCIÓN UNIVERSAL EN CIBERDELITOS EN LA LEGISLACIÓN ECUATORIANA

Línea de investigación:

DERECHO, PARTICIPACIÓN, GOBERNANZA, REGÍMENES POLÍTICOS E INSTITUCIONALIDAD

Autora:

Camila Salomé Paredes Robalino

Christian Danilo Gavilanes Domínguez, Ab. Mg f._____

CC. 1804630489

CALIFICADOR

Alex Marcelo Santamaría Navarrete, Ab. Mg. f._____

CALIFICADOR

Edgar Santiago Morales Morales, Ab. Mg. f._____

CALIFICADOR

Christian Danilo Gavilanes Domínguez, Ab. Mg. f._____

DIRECTOR ESCUELA DE JURISPRUDENCIA

Diego Danilo Coca Chanalata, Dr. f._____

SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Ambato – Ecuador

Febrero 2025

DEDICATORIA

A los que me aman incondicionalmente,

A ellos todo

- *Para Silvia y Vitaliano*

AGRADECIMIENTO

A Dios por tomarme de su mano, ser mi calma y mi guía.
A mis papis por apoyarme en mis objetivos y ser mi torre fuerte.
A mi familia, por demostrarme que siempre puedo volver a ellos.
A mis maestros, que con su paciencia forjaron mi profesión.
A mis compañeros, por su lealtad serán mis grandes colegas.
A mis amigos, por escucharme, apoyarme y animarme cada momento de la carrera.
A mi Federación de Estudiantes FEUCE, porque ahí encontré mi equipo increíble.

RESUMEN

La presente investigación resulta necesaria debido a la ausencia de regulación eficaz y actual en la legislación ecuatoriana respecto a la definición, el procesamiento y la imposición de sanciones de ciberdelitos. Esta carencia refleja sus consecuencias en la falta de claridad sobre la jurisdicción aplicable en casos de cibercrimen transnacional. Esta problemática ha permitido que un alto porcentaje de delitos cibernéticos queden impunes y la ciberdelincuencia se convierta en una de las principales actividades ilícitas más lucrativas del mundo.

Este estudio es importante para el Ecuador porque se plantean cuestiones esenciales para el combate contra la ciberdelincuencia en el país, y su debida aplicación en el marco normativo nacional. La presente tiene como objetivo principal analizar la jurisdicción universal en ciberdelitos en la legislación ecuatoriana. Para lograrlo, la metodología que se emplea es de tipo descriptivo, paradigma racional positivo, métodos deductivo, analítico y dogmático con un enfoque cualitativo y la aplicación de la modalidad bibliográfica-archivística; además de la utilización de entrevistas estructuradas a expertos del tema. De acuerdo con estas premisas, entre los resultados relevantes se establecen criterios jurídicos sobre la posibilidad de una jurisdicción universal en delitos cibernéticos en la legislación ecuatoriana para combatir de manera eficiente la ciberdelincuencia transnacional.

Palabras claves: jurisdicción universal, ciberdelitos, legislación ecuatoriana

ABSTRACT

The present research is necessary due to the absence of adequate and current regulations in Ecuadorian legislation regarding the definition, prosecution, and imposition of cybercrime sanctions. This lack reflects its consequences in the lack of clarity about the applicable jurisdiction in cases of transnational cybercrime. This problem has allowed a high percentage of cybercrime to go unpunished and cybercrime to become one of the most lucrative major illicit activities in the world. This study is vital for Ecuador because it raises essential issues for the fight against cybercrime in the country and its proper implementation in the national regulatory framework.

The main objective of this paper is to analyze the universal jurisdiction in Ecuadorian legislation regarding begrimes. To achieve this, the methodology used is descriptive, positive rational paradigm, deductive, analytical, and dogmatic methods with a qualitative approach. The bibliographic-archival modality is applied in addition to structured interviews with experts on the subject. According to these premises, among the relevant results, legal criteria are established on the possibility of universal jurisdiction in cybercrimes in Ecuadorian legislation to combat transnational cybercrime efficiently.

Keywords: *universal jurisdiction, cybercrimes, ecuadorian legislation.*

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La investigación analiza la jurisdicción universal en ciberdelitos en la legislación ecuatoriana para el debido procesamiento de estos delitos, debido a la naturaleza transfronteriza del ciberespacio. En primer lugar, el tema planteado es original puesto que, tras la búsqueda y examinación de bases de datos bibliográficas, plataformas y repositorios internacionales y nacionales, se observan investigaciones referentes a los procesos y determinación de la jurisdicción en delitos cibernéticos, pero no se plantea la iniciativa de la aplicación de una jurisdicción universal. Tras lo mencionado, en base a antecedentes investigativos existen tres estudios específicos, el primero en un ámbito internacional.

En el trabajo de Arrazola (2019) titulado “Conflictos de jurisdicción en materia de ciberdelitos: problemática y soluciones” se investiga acerca de la naturaleza del ciberespacio y los problemas que acarrea la carencia de límites físicos. Estos problemas del entorno cibernético son descritos en la no identificación del objeto, la transnacionalidad, la intangibilidad en la actividad investigadora y el conflicto de jurisdicciones. La metodología utilizada es bibliográfica de doctrina jurídica debido a que el autor expone la ausencia de actividad legislativa actual. Es a través de este trabajo donde se explican las posibles soluciones sobre el conflicto de jurisdicciones, si bien es cierto se menciona a la jurisdicción universal como una alternativa, pero la diferencia es que no ahonda en la aplicación práctica de la misma.

Desde el ámbito nacional, la autora Ochoa (2021) en su trabajo titulado “Desafíos globales del cibercrimen: caso Ecuador período 2014–2019” investiga el estado de varios países sobre el manejo de la ciberdelincuencia, además de la ejecución de políticas en ciberseguridad y de manera específica en el Ecuador analiza casos del periodo señalado para poder identificar los desafíos a futuro. A través de la metodología de derecho comparado de países de América Latina y el estudio de casos relevantes del Ecuador logra cumplir sus objetivos. Lo que diferencia a este estudio del presente es directamente el análisis de la jurisdicción en ciberdelitos en

primer lugar, si bien reconoce como desafío la multiplicidad de jurisdicciones, no ahonda en las posibles soluciones para delimitarla.

Por otro lado, de manera más específica el trabajo de Castillo (2024) titulado “Investigación de ciberdelitos como medio de tutela judicial efectiva” la autora enfatiza en el acceso a la justicia, la verdad procesal y la reparación integral en casos de ciberdelincuencia de manera que se proteja los derechos constitucionales durante todo el proceso en el Ecuador. Esto mediante una metodología tipo cualitativa y al utilizar métodos descriptivos y explicativos causales. Si bien es cierto, la autora analiza todo lo que conlleva un proceso de estos delitos en el Ecuador, pero lo que se diferencia del presente trabajo recae desde el inicio del proceso donde se delimita la jurisdicción en caso de aquellos transnacionales y con esto se tutela a la víctima de posibles vicios de nulidad.

La situación del problema se da por la creciente interacción del ser humano con la tecnología, sumado a la velocidad de invención de herramientas tecnológicas, actualmente utilizadas para cometer ciberdelitos, genera cada vez una brecha más profunda entre la realidad de la ciberdelincuencia y el marco jurídico que la combate. En la misma línea, factores como la naturaleza transfronteriza del ciberespacio, la multiplicidad de jurisdicciones, la falta de regulación específica y la complejidad de cumplir los procesos investigativos ha impedido que las autoridades pertinentes respondan de manera eficaz y coordinada a esta problemática.

La ciberdelincuencia es una de las mayores amenazas globales, debido a que los hábitos de la sociedad se trasladan al ciberespacio. De esta manera, los aspectos que miden esta problemática son, primero genera ingresos anuales que superan los cientos de miles de millones de dólares colocándose como una de las actividades más lucrativas a nivel mundial y segundo, ha puesto en desestabilización infraestructuras Estatales completas y vulnera derechos fundamentales de miles de personas.

Sumado a esto, gran cantidad de los ciberdelitos no son denunciados, esta subnotificación se da debido a algunos aspectos como el desconocimiento o la

desconfianza en las autoridades. Incluso existen casos que una vez denunciados, no siempre se obtiene una resolución debido a varios factores como la complejidad de los delitos, la pérdida de evidencia digital, la dificultad de localizar a los autores y los mecanismos de respuesta de los países. En esta misma manera, en un enfoque global la lucha contra la ciberdelincuencia encuentra un obstáculo en la divergencia de la normativa de los Estados y la falta de estándares comunes. Esto dificulta la investigación y sanción en delitos cibernéticos transnacionales, lo que fomenta la impunidad.

Una vez comprendido la gravedad de la problemática, el ciberespacio es el entorno global interconectado donde se desenvuelven las personas y redes digitales. Se enfatiza que este entorno no tiene fronteras geográficas, es decir, tiene una naturaleza transfronteriza porque precisamente esto plantea desafíos únicos. De esta manera, en el tema de delitos en el espacio cibernético la facilidad con la que los perpetradores operan a través de las fronteras obstaculiza la determinación de la jurisdicción de los Estados y a la par la eficiente investigación y sanción.

En cuanto el ciberespacio se identifica como una red de comunicación global pero la jurisdicción se basa mayormente en el principio de territorialidad de los Estados, surge la problemática bajo una ciberdelincuencia plurijurisdiccional. Esta se caracteriza por la divergencia entre el lugar donde se sitúa el equipo tecnológico, el lugar donde se controla el quipo por parte del responsable y el lugar donde se ve afectado el bien jurídico protegido. Por años, esta situación ha mantenido una baja actividad punitiva y/o reparadora por la concurrencia de diversos criterios sobre la instrucción del proceso y el alcance de la actividad investigativa de cada Estado sin llegar a fomentar una solución precisa.

El problema de investigación explicado se lo plantea de la siguiente forma: ¿En qué medida la aplicación de la jurisdicción universal contribuye a la efectiva persecución y sanción de los delitos cibernéticos en Ecuador?; A su vez, la hipótesis se desarrolla a través de la siguiente: La jurisdicción universal permite el procesamiento de los ciberdelitos en la legislación ecuatoriana.

El objetivo general de la presente investigación es analizar la jurisdicción universal en ciberdelitos en la legislación ecuatoriana. Para lograrlo los objetivos específicos se basaron en: 1. Fundamentar jurídica y doctrinariamente la jurisdicción universal y su aplicación en ciberdelitos en la legislación ecuatoriana. 2. Caracterizar a la jurisdicción universal en ciberdelitos en el territorio ecuatoriano. 3. Establecer criterios jurídicos sobre la posibilidad de una jurisdicción universal para los ciberdelitos en la legislación ecuatoriana.

En el trabajo se utiliza la metodología con enfoque cualitativo basado en el paradigma racional positivo para analizar la viabilidad en el Ecuador de combatir la ciberdelincuencia a través de la aplicación de la jurisdicción universal. Además, se usa un tipo descriptivo para presentar una imagen clara y completa del fenómeno o situación en particular y una modalidad bibliográfica para el estudio exhaustivo de fuentes documentales como normas tanto internacionales como nacionales, además de criterios jurisprudenciales y doctrina relevante sobre el tema y la revisión de casos prácticos.

Juntamente con la metodología, dentro de los métodos se utilizan el analítico y deductivo para comprender a detalle los elementos constitutivos de la jurisdicción universal y, además, comprender su aplicación en un entorno digital. En la misma línea, el método dogmático es de suma importancia para identificar lagunas en la normativa y buscar soluciones legislativas. Por último, se realizan entrevistas estructuradas a expertos en derecho penal y derecho digital, profesionales en ingeniería electrónica, sistemas y telecomunicaciones para que desde la perspectiva técnica y legal se dé una visión integral del problema y el desarrollo de la propuesta.

El presente trabajo resulta necesario porque en los últimos años la ciberdelincuencia se ha visualizado como una amenaza global y los esfuerzos por combatirla han resultado insuficientes, este tipo de delincuencia es de las actividades ilícitas más lucrativas del mundo que genera millones de dólares y esta investigación comprende la dimensión del problema para plantear criterios jurídicos que cooperen al combate contra la misma. Además, debido a la velocidad con la

que la tecnología y las herramientas electrónicas evolucionan y superan la capacidad de respuesta que tienen los Estados muchos perpetradores queden impunes y el presente trabajo investiga estos fenómenos.

Ante esta situación, la jurisdicción universal como el principio que combate la impunidad frente a delitos graves y complejos al permitir a los Estados juzgar a los responsables independientemente del lugar de comisión o la nacionalidad, se la presenta como una posible solución. La presente investigación busca analizar la viabilidad de esta herramienta en primer lugar en la legislación ecuatoriana y posteriormente al resto del mundo, debido a que esta jurisdicción, por eventos priores, se la conoce por enfrentar delitos graves que afectan a la globalidad de la población.

A través de esta investigación, se espera contribuir al combate de la ciberdelincuencia al analizar la realidad de la problemática, impulsar una adecuación o fortalecimiento de los marcos jurídicos sobre delitos informáticos, especialmente el del Ecuador y sentar bases con distintos países sobre la cooperación internacional efectiva. Los resultados de este estudio permitirán en primer lugar, el debate académico y político de una operación contra los ciberdelincuentes, además el planteamiento de reformas legislativas, distintas políticas públicas y de instrumentos internacionales para enfrentar en manera coordinada la amenaza global que representan el problema.

CAPITULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Acercamiento jurídico y doctrinario a los ciberdelitos

Desde la segunda mitad del siglo XX, como respuesta a una creciente interacción de las personas con la tecnología y distintas herramientas, surgen los ciberdelitos. Para Barrios & Marquéz (2024) "la ciberdelincuencia nace de la adaptación y mutación de diversas conductas delictivas del hombre a un entorno computacional y más recientemente a todo campo digital" (p. 535). De esta manera, la problemática mana en un contexto de interconexión global (Höffler & Sommerer, 2021), gracias a las computadoras y las redes digitales que se volvieron indispensables en todos los aspectos de la vida social, económica y política. En base a este antecedente, en una escala internacional este fue tema de interés a finales de los años 70 y comienzos de los años 80.

El hito importante internacionalmente fue en el año 1983, con la reunión de la Organización para la Cooperación y el Desarrollo Económico (OCDE). Es en este momento, por primera vez trataron la relevancia de la lucha contra los delitos informáticos a nivel global, y la transformación de los marcos normativos tradicionales por su falta de preparación para enfrentar las nuevas modalidades delictivas que trascendían fronteras (Barrios & Marquéz, 2024). De este modo, los países comenzaron a investigar, adaptar sus normativas y a firmar acuerdos multilaterales para ponerle fin a la ciberdelincuencia, como el Convenio de Budapest en 2001, el primer tratado internacional que aborda este tipo de delitos.

Como se ha visualizado a lo largo de la historia la ciberdelincuencia se ha posicionado como una de las mayores amenazas globales de este siglo. A la par de esto, si bien es cierto existen avances para combatir a los ciberdelincuentes, aun esta actividad es de las más lucrativas en el mundo, debido a que genera ingresos anuales que superan los cientos de miles de millones de dólares. En realidad, según estadísticas de Cybersecurity Ventures (2024) “si se midiera como país, entonces el cibercrimen (que se predice que causará daños por un total de 9,5 billones de dólares a nivel mundial en 2024) sería la tercera economía más grande del mundo

después de Estados Unidos y China, superando la riqueza de naciones enteras" (párr.1) de esto se desprende la constante evolución dañina de la problemática desde su origen.

Para continuar, de manera doctrinaria se define al ciberdelito. En relación con el presente estudio, Pastorini (2020) expone que "delito Informático, Ciberdelito, o Cibercrimen, es entendido como aquella conducta típica, antijurídica y culpable, cuyo medio de comisión o cuyo objeto es la informática" (p.3). De esta manera, estos ilícitos se caracterizan por el uso inadecuado de los medios tecnológicos, donde computadores o dispositivos móviles son herramientas para cometer actividades delictivas. Es posible observar que, la cibernética también ha facilitado el cometimiento de delitos tradicionales, como aquellos que afectan al patrimonio o al honor de las personas, sean más accesibles para los perpetradores, debido al uso de instrumentos tecnológicos (Tapia, 2022). Comprendido esto, existen ciertas características generales.

Si bien es cierto, existe un daño ocasionado por el cometimiento tanto de delitos tradicionales como de ciberdelitos, estos difieren por el entorno en el que ocurren y cómo se llevan a cabo. Es por tal motivo que, Cueva & Tapia (2022) exponen distintas características: "se cometen con facilidad, necesitan pocos recursos en comparación con el perjuicio que causan; se cometen en una jurisdicción sin estar físicamente en el territorio donde originan el daño y estos encuentran lagunas de punibilidad en varias legislaciones" (p. 19). Tras esto, se verifica la necesidad de profundizar en la operatividad de este tipo de delitos.

El ciberdelito opera mediante la explotación de vulnerabilidades en sistemas informáticos o dispositivos conectados a internet, con la finalidad de dañar, robar o únicamente acceder a la información sin una autorización correspondiente. Para Guzmán, Palacios, & Palacios (2023) "son actividades como la creación y propagación de malware, piratería informática usada para robar datos personales o industriales sensibles y ataques de denegación de servicio para causar daño financiero y/o reputacional" (p.531). Se comprende entonces que el delito cibernético tiene como objetivo directo los entornos digitales, ya sea atacar

infraestructura tecnológica o manipular datos en línea. La Interpol (2021) expone que incluyen la propagación de virus u otro malware, piratería y ataques de denegación de servicio distribuida (DDoS), además de técnicas avanzadas, como *malware, phishing, ransomware*.

Por consiguiente, existen varios autores que identifican a los ciberdelitos como ilícitos tradicionales en el que se utilizan medios informáticos, sin reconocer un bien jurídico autónomo. Por el contrario, autores como Saltos, Robalino, & Pazmiño (2021) argumentan que los delitos informáticos tienen un contenido propio, que afecta un nuevo interés social que requiere reconocimiento legislativo. Para este punto, cabe profundizar sobre la diferenciación de un delito informático y un delito cometido por medios informáticos.

En base a la información de la Interpol, se distinguen ciertas particularidades. En primer sentido, un delito informático es aquel que únicamente se comete al utilizar Tics o las denominadas tecnologías de la información y la comunicación, además estos delitos no existen fuera de la tecnología por ejemplo piratería, virus o propagación de malware, ataques de denegación de servicio distribuida. En otro sentido, el delito cometido por medios informáticos son aquellos delitos comunes o llamados tradicionales que tienen la capacidad de aumentar su alcance mediante el uso de las Tics.

Internacionalmente la determinación del bien jurídico protegido en los ciberdelitos ha sido objeto de debate. En primer lugar, se define a este como el bien lesionado por el actuar del sujeto activo. Consecuentemente, existen diferentes puntos de vista debido a la premisa que cualquier bien jurídico es afectado por medios electrónicos, y en la otra posición de que este es delimitado. De esta manera, en los delitos informáticos, el bien jurídico protegido depende del interés afectado o puesto en riesgo por la acción delictiva, sin embargo, existe una disputa sobre si lo que se protege son los datos o la información de los sistemas informáticos (Cornejo, 2021). En la misma línea, Acurio del Pino (2016) menciona que el bien jurídico protegido es la información en sí; esta no es gestionada de la misma manera que los bienes materiales, pero la importancia recae en su valor económico.

Si bien es cierto que se protege la información en todo su sentido, también se protegen varios bienes jurídicos como el patrimonio, la privacidad de los datos, la seguridad jurídica y el derecho de propiedad. En la misma línea, el Convenio sobre Ciberdelincuencia divide a estos bienes en cuatro grupos, aquellos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos como relacionados con intereses propiamente informáticos. De esto se comprende que, los bienes jurídicos protegidos se agrupan, pero depende de cada delito en particular para poder delimitar el derecho que se tutela.

A propósito de lo mencionado y al verificar el contexto de la revolución tecnológica, principalmente de la globalización, se forma la delimitación de los derechos humanos de quinta generación, que también son tutelados por la tipificación de los ciberdelitos. En esta categoría principalmente se encuentran aquellos derechos vinculados con el acceso a las nuevas tecnologías de la información y la comunicación. Además, se vela específicamente sobre la ciberseguridad y la protección de datos personales. Se considera como derechos humanos a algunos como la privacidad digital y la protección de datos personales. Estos derechos se protegen para que las personas ejerzan su libertad fundamental en el ciberespacio, además de no ser víctimas de delitos informáticos que violen su privacidad, información o patrimonio.

En consecuencia, para estudiar los ciber punibles en el ámbito penal, conviene entender su concepción en las distintas legislaciones y la comparación es el medio apropiado (Martins, 2022). En el apartado siguiente, se reflejan las conductas punibles por vía del derecho comparado entre regímenes de los países de Colombia, Perú y Chile quienes, tras identificar la problemática en la región, ratifican instrumentos internacionales y posteriormente en su legislación interna promulgan leyes específicas para abordar los delitos cibernéticos. Estos países son tomados en cuenta para el presente trabajo por similitudes culturales y legales, experiencias regionales, la existencia de estadísticas de ciberdelincuencia en América del Sur y el accionar Estatal de manera internacional y nacional.

Tabla 1. Ciberdelitos Derecho Comparado Perú, Colombia y Chile

Ítem de comparación	Perú	Colombia	Chile
Estadísticas de Ciberdelitos	En el estudio realizado la Defensoría del Pueblo de Perú en el año 2023, se demuestran varios resultados, las denuncias del año 2018 al año 2021 se cuadruplicaron. En el año 2021 se tuvo más de 12.000 denuncias de ciberdelitos, esto con proyección a los siguientes años se considera un incremento significativo.	El estudio realizado por el Tanque de Análisis y Creatividad de las TIC de Colombia sobre ciberdelitos en el año 2023 expone que en el año 2020 el año de pandemia los ciberdelitos denunciados fueron 22.000 mientras que en el año 2022 estos llegaron a 14.000 denuncias. Los sectores más afectados fueron industrias, gobierno, salud y educación.	En el estudio presentado por la Policía de investigaciones Chile en 2022 y EMB en el año 2024 se destaca la preocupación del Estado por los ciberdelincuentes que en el en un periodo de un año, de agosto del 2022 a agosto del 2023 cada minuto el país sufrió 27 ataques cibernéticos. Además, que más del 90% de las organizaciones del país no están preparadas para afrontar esta delincuencia.
Normativa Internacional ratificada por el país	Si: Convenio de Budapest es aprobado mediante Resolución Legislativa No. 30913, del 12 de febrero de 2019.	Si: Colombia se adhiere al Convenio de Budapest en el año 2020.	Si: Chile ha ratificado el Convenio de Budapest en el año 2017, este fue aprobado en el Decreto 83.
Normativa interna que regulen los ciberdelitos	Si: dentro de la legislación se expone la Ley N°29733, que conlleva temas de ciberdelitos, además de otras leyes complementarias al campo como la Ley de Protección de Datos Personales, la Ley Nº 30096, Ley de Delitos Informáticos	Si: La Ley 1273 de 2009 complementa el Código Penal sobre la ciberdelincuencia.	Si: Chile cuenta con la Ley 21459, esta se da en 2022, cuando adapta su legislación interna luego de haber ratificado el Convenio de Budapest. Además, cuenta con leyes como Telecomunicaciones, Responsabilidad Penal de Personas Jurídicas y Protección de Vida Privada.

Fuente: elaboración propia modificado a partir de Mejía, Hurtado, & Grisales (2023)

De esta síntesis de la situación actual en ciberdelitos en los diferentes países, se destaca que los tres Estados en los últimos 5 años han sido víctimas de delincuentes cibernéticos y su proyección aumenta. Además, los sistemas han ratificado normativa internacional que regula esta clase de crímenes. Por un lado, han experimentado un desarrollo significativo, donde la normativa opera y se acopla al Convenio sobre la ciberdelincuencia, en donde se tipifican nuevos delitos como ataques informáticos, falsificación y fraude. Además de eso, no solo se añaden nuevos tipos penales en las leyes, sino que a la actualidad se han regulado los procesos investigativos y sancionatorios de manera interna.

Para ejemplificar la operatividad y alcance de los ciberdelitos se destacó la Operación KAERB. Gracias a datos de la Agencia de la Unión Europea para la Cooperación Policial (Europol), Comunidad de Policías de América (Ameripol) y noticias de la Fiscalía General del Estado ecuatoriano, una red internacional de delitos informáticos actuaba en España, Colombia, Argentina, Perú, Chile y Ecuador. Aquella empleaba técnicas de ingeniería y malware para cometer delitos como robo de terminales móviles, robo de datos, acceso indebido, extorsiones y fraude. En la misma línea “a través de una plataforma digital denominada iServer, que operaba bajo múltiples dominios y utilizaba métodos de pago anónimos, y generaba mensajes de phishing para obtener las credenciales de acceso de las víctimas” (Fiscalía General del Estado, 2024, párr. 2). Este operativo fue exitoso en el Ecuador en el año 2024, tras años de investigación.

En base a este caso, se observa la magnitud del daño causado por la ciberdelincuencia. Debido a que “esta red de criminales operó hace cinco años, además mantenía alrededor de 2.000 usuarios registrados y un estimado de 483.000 víctimas en países como Chile (77.000), Colombia (70.000), Ecuador (42.000), Perú (41.500), España (30.000), Argentina (29.000) y otros (193.500)” (Fiscalía General del Estado, 2024, párr. 5). Tras la detención de 17 responsables en todo el operativo, y al ser un caso actual, aún se espera el proceso judicial de cada uno, debido a la existencia de 8 nacionalidades distintas.

Como esta operación, en los últimos años alrededor del mundo se han dado varios eventos delincuenciales en la red. Para la comprensión del alcance de los ciberdelitos se destaca la siguiente tabla de incidentes ocurridos en el año 2024 en distintos países:

Tabla 2. Incidentes Cibernéticos Significativos

Fecha	País/Países	Descripción
11/2024	Reino Unido	El Centro Nacional de Seguridad Cibernética del Estado describió que en comparación al año 2023 los ciberataques incrementaron tres veces y las amenazas reales para este Centro son países con alto desarrollo tecnológico como Rusia, Irán y China mediante mecanismos inteligentes.
10/2024	Rusia Ucrania	Agentes de Rusia mediante el uso de correos electrónicos amenazaron a embajadas ucranianas sobre la explosión de bombas en las instituciones y agencias estatales.
08/2024	Estados Unidos	Dentro de la campaña presidencial de Donald Trump, los funcionarios estatales detectaron que piratas informáticos iraníes de irrumpir y ofrecer compartir documentos robados de la campaña.
03/2024	Suiza	El Centro Nacional de Seguridad Cibernética (NCSC) tras un proceso legal confirmó que en mayo del año 2023 los datos que fueron sustraídos incluían documentos personales, información clasificada de la Administración Federal.

Fuente: elaboración propia modificado a partir de Center For Strategic & International Studies (2024)

Tras lo investigado acerca de la regulación de ciberdelitos alrededor del mundo. Cabe resaltar que, en el contexto ecuatoriano, la Constitución de la República del Ecuador no aborda específicamente estos delitos. Si bien es cierto se mencionan distintos bienes jurídicos protegidos conexos, como el acceso universal a las tecnologías de información y comunicación y el derecho a la intimidad personal y familiar; no es menos cierto que, a pesar de la existencia de normas internacionales como se visualizó en la tabla 1, el Estado Ecuatoriano según la Fiscalía General del Estado internacionalmente ha ratificado algunos únicamente referente a derechos de autor y las telecomunicaciones.

De este contexto internacional y constitucional, conviene estudiar a profundidad el Código Orgánico Integral Penal, toda vez que en este se encuentran tipificados todos los delitos. Si bien es cierto, no hay una normativa en específico que delimite los delitos cibernéticos punibles en el país, ni han existido reformas para la debida adaptación de la normativa a los estándares internacionales. En la misma línea, lo mencionado limita la capacidad del sistema judicial en responder frente a estos casos, se fomenta a un desfase entre la legislación y la realidad y se pone en riesgo la seguridad cibernética del Estado. A continuación, se presenta una tabla de lo que considera actualmente el país ciberdelitos en las siguientes figuras del COIP.

Tabla 3. Ciberdelitos en el Código Orgánico Integral Penal

Artículo COIP	Delito	Pena Privativa de Libertad
Art. 91	Trata de personas	De 16 a 19 años.
Art. 100	Explotación sexual de personas	De 13 a 16 años.
Art. 103	Pornografía con utilización de niñas, niños o adolescentes	De 13 a 16 años.
Art. 104	Comercialización de pornografía con utilización de niñas, niños o adolescentes	De 10 a 13 años.
Art. 154	Intimidación	De 1 a 3 años.
Art. 166	Acoso sexual	De 1 a 5 años.
Art. 168	Distribución de material pornográfico a niñas, niños y adolescentes	De 1 a 3 años.
Art. 172	Utilización de personas para exhibición pública con fines de naturaleza sexual	De 7 a 10 años.
Art. 173	Contacto con finalidad sexual con menores de dieciocho años por medios electrónicos	De 1 a 3 años.
Art. 174	Oferta de servicios sexuales con menores de dieciocho años por medios electrónicos	De 7 a 10 años.
Art. 178	Violación a la intimidad	De 1 a 3 años.
Art. 186	Estafa	De 5 a 7 años.
Art. 190	Apropiación fraudulenta por medios electrónicos	De 1 a 3 años.
Art. 191	Reprogramación o modificación de información de equipos terminales móviles.	De 1 a 3 años.
Art. 192	Intercambio, comercialización o compra de información de equipos terminales móviles	De 1 a 3 años.
Art. 193	Reemplazo de identificación de terminales móviles.	De 1 a 3 años.
Art. 194	Comercialización ilícita de terminales móviles	De 1 a 3 años.
Art. 211	Supresión, alteración o suposición de la identidad y estado civil	De 1 a 3 años.
Art. 212	Suplantación de identidad	De 1 a 3 años.
Art. 229	Revelación ilegal de base de datos	De 1 a 3 años.
Art. 230	Interceptación ilegal de datos	De 3 a 5 años.
Art. 231	Transferencia electrónica de activo patrimonial	De 3 a 5 años.
Art. 232	Ataque a la integridad de sistemas informáticos	De 3 a 5 años.
Art. 233	Delitos contra la información pública reservada legalmente	De 5 a 7 años.
Art. 234	Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.	De 3 a 5 años.
Art. 298 Inciso 8	Defraudación tributaria: Alteración de libros o registros informáticos de contabilidad	De 1 a 3 años.
Art. 323	Captación Ilegal de Dinero	De 5 a 7 años.

Fuente: elaboración propia modificado a partir de Quezada, y otros (2022) y Código Orgánico Integral Penal [COIP] (2024)

Tras lo estudiado, los ciberdelitos y conexos están tipificados en la legislación ecuatoriana dentro de su normativa interna, específicamente en el Código Orgánico Integral Penal. Este marco legal refleja los esfuerzos por abordar los desafíos que la era digital presenta. De igual manera en el país, la Fiscalía General del Estado creó la unidad especializada para investigar estos delitos, en la resolución No. 34-FGE-2022 se especifican los que se consideran delitos informáticos como son la revelación ilegal de base de datos, interceptación ilegal de datos, transferencia

electrónica de activo patrimonial, ataque a la integridad de sistemas informáticos, delitos contra la información pública reservada legalmente, acceso no consentido a un sistema informático, telemático o de telecomunicación, y la pornografía con utilización de niñas, niños o adolescentes y su comercialización.

En el país la comprensión de la gravedad de la ciberdelincuencia es difícil porque las únicas cifras, alarmantes, pero no cercanas a la realidad, que se tienen por parte del Ministerio del Interior (2023) señalan que “en 2020 se presentaron 562 denuncias por ciberdelitos, en 2021 fueron 849 y en 2022, 831, mientras que los delitos cometidos a través de las TIC registraron las siguientes cifras: 2020, 9.656; 2021, 14.714 y el año pasado 12.939” (párr.4). Tras lo estudiado la falta de datos precisos, actualizados y confiables sobre los casos de delitos cibernéticos sancionados es un obstáculo significativo para tomar acción, además del previo conocimiento que varios delitos llegan a denunciarse, pero estos no son sancionados.

De esto también se subsume que, al no existir una evaluación certera de la situación actual, esta problemática no ha sido visible para autoridades que son los encargados de que se tome acciones definitivas en la lucha contra la ciberdelincuencia, sino que por el contrario esta ha permanecido subestimada en el Ecuador. Por último, cabe señalar que, al observar estadísticas globales y estadísticas de países aledaños, las cifras de delincuencia cibernética son impresionantes y el Estado ecuatoriano no está exento de estas.

1.2. Delimitación normativa de la jurisdicción universal

Al empezar, es menester conceptualizar a la jurisdicción como la autoridad legal otorgada a los tribunales para resolver conflictos y hacer cumplir sus decisiones dentro de un territorio específico. Doctrinariamente, Escriche (1869) define a la jurisdicción como:

> El poder o autoridad para gobernar y poner en ejecución las leyes; y especialmente la potestad de que se hallan revestidos los jueces para

> administrar justicia, o sea para conocer de los asuntos civiles o criminales o así de unos como de otros, y decidirlos o sentenciarlos a las leyes (p.1113).

Además de esto, el núcleo central de la jurisdicción es determinar el hecho alegado sometido a juicio, y la aplicación debida del derecho para la resolución (Baltán, 2022).Tras aquello, se comprende que la jurisdicción limita el conocimiento de las causas judiciales, garantiza el orden y la justicia dentro del marco legal establecido.

Ahora bien, al comprender doctrinariamente la jurisdicción cabe profundizar su definición en base a la jurisprudencia, además ampliar sobre la distinción de jurisdicción y competencia, la Corte Constitucional del Ecuador (2007) explica que la jurisdicción es:

> El poder genérico de administrar justicia, dentro de los poderes y atribuciones de la soberanía del Estado; y la competencia es precisamente el modo o manera como se ejerce esa jurisdicción por circunstancia concretas de materia, grado, y territorio, imponiéndose por tanto una competencia, por necesidades de orden práctico (Resolución No. 0152-07-HC, 2007).

De esta forma, la competencia delimita las funciones concretas de cada órgano judicial, entiéndase como una especialización dentro de la jurisdicción.

Comprendida la definición de jurisdicción y competencia, en base a varios autores se expone que, en materia penal, la medida de la justicia se ha basado mayormente en el principio de territorialidad. Así lo mencionan Pino, Rojas & Copa (2021) el principio establece que la legislación penal se aplica únicamente a los delitos cometidos dentro del territorio de un Estado. Esto significa que los Estados tienen el derecho de ejercer su jurisdicción sobre los delitos ocurridos en su territorio, así como en los barcos y aviones registrados en aquel Estado.

Por otro lado, ciertos autores de doctrina penal internacional han delimitado también el principio de ubicuidad. Este principio menciona que un delito se considera no solo

cometido en el lugar de los resultados, sino en absolutamente todos los lugares en los que se ha desarrollado la conducta como la fase de ejecución. Además, se lo reconoce en el Derecho Internacional por la jurisprudencia de la Corte Penal Internacional y la sentencia Lotus de la Corte Permanente de Justicia Internacional de 1927 así el ilícito se comete en todos los lugares en los que se cumplen los elementos de un tipo penal nacional (Payer, 2024). Cabe destacar este principio que, por su incidencia transfronteriza forma parte de los criterios para delimitar la jurisdicción de un Estado. Es así como se desprende la interrogante de la regulación de la jurisdicción en el territorio ecuatoriano.

En Ecuador, la jurisdicción está regulada por el Código Orgánico Integral Penal, en el artículo 400. Donde se menciona, en primer lugar, cualquier ecuatoriano o extranjero que cometa una infracción dentro del territorio nacional. En segundo lugar, la jurisdicción se extiende a jefes de Estado, representantes diplomáticos del Ecuador, así como a cónsules ecuatorianos, cuando estos cometen infracciones en el extranjero en el ejercicio de sus funciones. Además, se incluyen infracciones cometidas por ecuatorianos o extranjeros a bordo de naves aéreas o marítimas de bandera ecuatoriana, ya sea en espacio aéreo nacional, mar territorial ecuatoriano, o en el espacio aéreo o mar territorial de otro Estado. También, para ecuatorianos o extranjeros que cometen infracciones contra el derecho internacional o derechos previstos en tratados internacionales vigentes, sino son juzgados en otro Estado.

Al comprender el tema de la jurisdicción en base al principio de territorialidad en la legislación ecuatoriana, se da paso al estudio de lo que conlleva una jurisdicción universal. Como se ha observado con anterioridad, la jurisdicción se basa en una manifestación de la soberanía estatal, esto en conjunto mayormente con el principio de territorialidad, limita a la jurisdicción a las fronteras de cada país a menos que se refiera a la jurisdicción universal.

La jurisdicción universal tiene una definición importante para el derecho internacional penal porque esta es aquella que permite que un Estado ejerza su autoridad legal y sancione algunos delitos independientemente del lugar de cometimiento o la nacionalidad de las partes. Es así como Pino, Rojas & Copa

(2021) exponen que esta jurisdicción “cobra vida cuando se aplica la ley punitiva fuera del territorio de una nación, esto permite ampliar la jurisdicción más allá de sus límites materiales" (p.9). De esta manera, la jurisdicción universal se caracteriza por permitir a los tribunales de cualquier país perseguir, sancionar los delitos y contribuir a la lucha contra la impunidad.

La jurisdicción universal recae en un mecanismo jurídico para combatir la impunidad en relación con crímenes graves que afectan a la humanidad. Esta se fundamenta en normas internacionales como el *Ius Cogens*, que reconoce estos delitos como una amenaza para la comunidad internacional (Rodriguez & Méndez, 2023). En la misma línea, al sustraerse a la jurisdicción nacional los crímenes *delicta iuris gentium* es decir, delitos contra el derecho de gentes, adquieren una dimensión universal debido al gran daño que causan a la comunidad internacional.

Además de las características mencionadas, Erique-Zambrano (2022) caracteriza a la jurisdicción universal como aquella utilizada para “velar por los intereses de la comunidad internacional en no permitir la impunidad y en ayudar a juntar fuerzas entre los estados en su persecución” (p. 614). Esta jurisdicción comúnmente es aplicada en el Derecho Internacional para sancionar crímenes graves como genocidio y crímenes de guerra, pero actualmente en base a la amplia gama de delitos transnacionales y la grave afectación a la comunidad global, los países consideran crucial la cooperación internacional y la aplicación de la jurisdicción universal en algunos campos.

Si bien es cierto, la jurisdicción universal encuentra su origen en la persecución marítima de piratas hace varios siglos atrás. Por un lado, su fuente oficial son los juicios de Nuremberg, seguido por el amplio desarrollo del derecho penal internacional, debido a que es la manera conocida actualmente para juzgar los crímenes de lesa humanidad (Pino, Rojas, & Copa, 2021). Además, esta jurisdicción ha evolucionado con la idea de que ciertos crímenes son tan graves que trascienden las fronteras nacionales y, por lo tanto, justifican la intervención de cualquier Estado para garantizar el cumplimiento del derecho internacional (Erique-

Zambrano, 2022). En base a esto, las faltas juzgadas en base a la jurisdicción universal se han ampliado como es el Caso de Pinochet.

Augusto Pinochet fue el actor principal de un hito en la historia de jurisdicción universal. El ex dictador de Chile en el año 1973 encabezó un golpe de Estado donde instauró una dictadura militar, en este periodo se dan graves violaciones de derechos humanos a toda la comunidad chilena. Es de conocimiento que, al final de la dictadura, Pinochet entrega el poder y termina la dictadura en Chile, a la vez que se le otorga inmunidad en el país con un acuerdo previo bajo esos términos. En el año 1998 el gobierno español solicita formalmente a las autoridades británicas, donde Pinochet se encontraba, que sea extraditado a España (Poó-Figueroa, 2024). Tras estos hechos se inicia el debate acerca de la aplicación de la jurisdicción universal, debido a la inmunidad que gozaba Pinochet en Chile. Se dictamina que el exdictador no era inmune para la jurisdicción española y convenia juzgarlo por los crímenes, así lo expone la Cámara de Lores británica.

Tras este caso, otro caso importante fue el de Julian Assange. Como lo relata Hernández (2024) en el año 2010, WikiLeaks donde Assange estaba a cargo, publicó varios documentos clasificados del Ejército de Estados Unidos. En los documentos tenía según BBC News Mundo (2019) “cuatrocientos mil reportes sobre la guerra de Irak, 90.000 sobre la guerra en Afganistán, 800 desde la prisión de Guantánamo y más de 250.000 cables diplomáticos redactados en varias partes del mundo” (párr. 1). Tras este suceso, al mismo tiempo Suecia emitió contra Assange una orden de detención debido al presunto cometimiento de delitos sexuales.

En cuanto al proceso de Suecia, Assange negó los argumentos y alegó que la controversia es de naturaleza política. Assange solicitó asilo político en Ecuador, este fue conferido y evita ser extraditado a Suecia por el proceso de delito sexual. En el año 2019 Ecuador le retiró el asilo y él fue detenido por la policía británica. A la par de esto, Estados Unidos en base a su jurisdicción, pidió que lo extraditen para que enfrente los cargos por la filtración de documentos clasificados. Esto

concluyó cuando Assange aceptó un acuerdo con el Departamento de Justicia de Estados Unidos para cumplir con su condena.

Tras la ejemplificación mediante dos casos emblemáticos, cabe destacar la utilización de la jurisdicción universal. Por un lado, la constante evolución del derecho internacional, la necesidad de combatir la impunidad, la protección integral de los derechos humanos y la necesidad de completar otros mecanismos como asistencia mutua, ha llevado a que algunos Estados consideren la aplicación de la jurisdicción universal fuera de su ámbito tradicional de funcionamiento. Tras lo expuesto, este principio tiene incidencia en la normativa del Ecuador.

En la legislación ecuatoriana, la jurisdicción universal se encuentra respaldada desde la Constitución de la República del Ecuador. Es de esta manera que, la Constitución en su artículo 416, establece la promoción y defensa de los derechos humanos y el derecho internacional como principios rectores de su política exterior. En la misma línea, el COIP en su Artículo 400, regula la potestad jurisdiccional penal de Ecuador, donde especifica que las y los ecuatorianos o extranjeros que cometan infracciones contra el derecho internacional o los derechos previstos en convenios o tratados internacionales vigentes están sujetos a la jurisdicción penal ecuatoriana, siempre que no hayan sido juzgados en otro Estado.

Por otro lado, en el mismo cuerpo menciona que la jurisdicción universal para los delitos contra la humanidad o de lesa humanidad. Esto significa que dichos crímenes son investigados y juzgados en el territorio ecuatoriano, siempre que no hayan sido previamente juzgados en otro Estado o por cortes penales internacionales. La normativa se aplica en conformidad con el COIP y los tratados internacionales (Código Orgánico Integral Penal, art. 401).

1.3. Jurisdicción universal en ciberdelitos

Una vez entendida la jurisdicción universal, cabe resaltar que los ciberdelitos se desenvuelven en un ciberespacio. Este es entendido como un dominio digital global e interconectado que engloba redes, sistemas y tecnologías de la información

(Bartolomé & Monteiro, 2021). Este entorno virtual en constante evolución facilita la comunicación, el intercambio de datos y la realización de diversas actividades a escala mundial. Es necesario agregar que este espacio no está limitado por fronteras geográficas (Gil, 2023); además Corozo (2024) expone que “en el ciberespacio se ha enfrentado desafíos legales relacionados con la privacidad, la seguridad cibernética, la protección de datos y la responsabilidad de los actores estatales y no estatales” (p.221). Se expone entonces que la naturaleza transfronteriza del ciberespacio desafía los conceptos tradicionales de jurisdicción.

La naturaleza transfronteriza del ciberespacio es lo que lo sitúa más allá de las jurisdicciones nacionales, convirtiéndolo en un escenario de interacción compleja entre actores estatales y no estatales. También, casi siempre obedecen a temporalidades más audaces que las de las normas y los procedimientos que los combaten (Vinelli, 2021). De este punto se desprende que los ciberdelitos al tratarse de conductas que ocurren en el ciberespacio son de difícil localización en los espacios territoriales de cada uno de los Estados lo que limita el nivel de respuesta de los sistemas jurídicos.

Tras la exposición de la naturaleza transfronteriza del ciberespacio, cabe indagar acerca de los problemas de jurisdicción al momento de las diligencias investigativas en ciberdelitos, como la concurrencia de jurisdicciones. El problema que se trata se da debido a la naturaleza expuesta de los ciberdelitos, donde los perpetradores, equipos y víctimas están dispersos en múltiples jurisdicciones. Además, para Corozo (2024) “los delitos cibernéticos pueden originarse en un país, afectar a otros y utilizar infraestructuras ubicadas en múltiples jurisdicciones” (p. 224). Debido a esto, uno de los mayores retos para los países recae en regular la jurisdicción en ciberdelitos.

Además, factores específicos del ciberespacio como el desarrollo apresurado de herramientas y tecnologías, sumado el anonimato y la dificultad de atribuir actividades a perpetradores determinados han sido los principales obstáculos para perseguir y sancionar a ciberdelincuentes (Valencia, 2024). En concordancia con esto, organizaciones internacionales de policía como la Interpol y la Europol

recalcan la complejidad en delimitar la jurisdicción en la esfera internacional en ciberdelitos porque estos no conocen fronteras y existe impunidad en distintos casos. Por ejemplo, la Europol en su lucha por erradicar la ciberdelincuencia creó el Centro Europeo de Ciberdelincuencia EC3, donde estrecha fuerzas policiales europeas con apoyo técnico 24 horas al día, así se llevan a cabo procesos investigativos e incentiva la cooperación internacional.

Tabla 4. Desafíos de determinar la jurisdicción en el ciberespacio

Múltiples jurisdicciones	**Marcos legales convergentes e inadecuados**	**Rápido desarrollo de tecnología y conductas delictivas**
Para explicar este desafío se plantea un caso hipotético. Un ciberdelito se comete desde un país, utiliza servidores de otro y quienes son los afectados o víctimas se encuentran en un tercer país, entonces es complicado determinar la jurisdicción. Gracias a la naturaleza transfronteriza del ciberespacio lo que ocurre en este entorno no está limitado por fronteras físicas y varios países están facultados para investigar y juzgar los delitos, esto sin la debida coordinación internacional fomenta la impunidad.	Para explicar este desafío se plantea una metáfora. Este entorno cibernético que es una autopista internacional sin señales de tráfico claras. En un momento dado, un carro choca con otro por la velocidad a la que iba, pero para la perspectiva del primer carro no tiene culpa porque respetaba sus reglas nacionales, entonces como se soluciona sin un marco legal en común. Entendido esto, cuando cada Estado tiene su propia normativa penal con definiciones y sanciones distintas para ciberdelitos, además de que no existen acuerdos sólidos para la correcta cooperación internacional, se dificulta la persecución de delitos por los conflictos de jurisdicción de cada país.	El ciberespacio consta de un entorno de computadores e individuos que han trasladado su cotidianidad y costumbres a la red. En base a esto, la sociedad cada día se transforma y se desarrolla de manera acelerada e intercomunicada a nivel mundial. El problema de las leyes es que cumplen un proceso muchas veces largo, entonces algunas de estas fueron creadas hace años y la rapidez de la tecnología causa que actualmente sean obsoletas, cuando estas se actualicen, ya existen nuevas modalidades y herramientas. Así**,** aunque el derecho sea cambiante, es un proceso más lento al de la sociedad.

Fuente: elaboración propia

En base a lo mencionado, se considera a uno de los organismos internacionales para conocer acerca de la jurisdicción universal en ciberdelitos. La Corte Penal Internacional (CPI) quien se centraba exclusivamente en los crímenes de guerra y de lesa humanidad establecidos de forma exhaustiva en su Estatuto, en el año 2023 tras sufrir un ciberataque a sus sistemas expone su preocupación y su compromiso de sancionar este tipo de actos. De esta forma, se da un paso amplio al principio de universalidad en ciberdelitos, debido al Estatuto de Roma donde se menciona que estos delitos graves se adaptan a nuevas formas de conflicto como aquellas dentro del ciberespacio. En la misma línea, en base al contexto y el alcance de los

delitos cibernéticos la normativa de la CPI los considera cibercrímenes de guerra y quien conviene que juzgue estos independientemente de donde se realizaron los actos es la CPI.

Para este punto, cabe ampliar sobre los convenios internacionales que regulan de distintas maneras los ciberdelitos, como es el Convenio de Budapest. Es el primer tratado internacional que lucha contra la ciberdelincuencia, este fue firmado en 2001 por el Consejo de Europa (Becker & Viollier, 2020). En este Convenio existe el apartado de jurisdicción, es ahí donde se establecen tres tipos de jurisdicción. En primer lugar, la jurisdicción es del Estado si el delito es cometido en su territorio, en segundo lugar, la jurisdicción es del Estado cuando el delito es cometido por uno de sus nacionales, independientemente de donde se haya cometido el ilícito, por último, la jurisdicción la tiene un Estado si el delito afecta a un interés legítimo de ese Estado, cabe la integridad territorial como la seguridad nacional. Tras esto, el Convenio amplió las posibilidades de que el Estado juzgue un ciberdelito, incluso si este no fue cometido dentro de sus límites territoriales.

Tras lo expuesto, dentro del Convenio se menciona de igual manera, el principio de asistencia mutua, donde en base a la cooperación internacional cada uno de los Estados se comprometen a brindar su apoyo, en acciones como compartir información, localizar sospechosos, ejecutar órdenes judiciales, obtener pruebas, entre otros. Dentro de los avances en la lucha contra la ciberdelincuencia que ha traído este Convenio, se visualiza por las operaciones como Cloud Hopper que el principio de asistencia mutua es utilizado al momento de perseguir el cometimiento de un ciberdelito que incluye a varios Estados.

Desde otra perspectiva, está la Convención contra la Ciberdelincuencia de la Asamblea General de las Naciones Unidas expuso su primer borrador en el año 2024 y se abrirá a la firma en los próximos años. Es un instrumento internacional que tiene por finalidad combatir la delincuencia cibernética. En base al borrador de este, se plantean definiciones claves sobre los delitos, además la importancia de la cooperación internacional. Lo importante hay que destacar es que aún persisten

incertidumbres sobre cómo se aplicará distintos puntos de esta convención a un entorno digital transfronterizo.

Es menester profundizar sobre la armonización de la normativa interna de los Estados frente al Convenio de Budapest y sus protocolos adicionales. Cabe aclarar que, el primer protocolo del año 2003 versa sobre la tipificación penal de actos racistas y xenófobos cometidos en sistemas informáticos, y consecuentemente el segundo protocolo del año 2022 recae sobre nuevas medidas de cooperación internacional (Hertler, 2024). Actualmente, en la legislación ecuatoriana este Convenio fue ratificado en el mes de julio del año 2024, es decir, es necesaria la armonización de la normativa interna sobre la definición de delitos cibernéticos y el compromiso de la cooperación internacional.

Si bien es cierto que el cuerpo normativo es el más relevante en la materia, este ha quedado obsoleto en algunos aspectos, debido a nuevas modalidades, conductas y herramientas que han surgido desde su adopción, como casos graves a escala global de ransomware que afectaron a múltiples países y no han tenido una verdadera investigación y sanción. Así los aspectos que no fueron tomados en cuenta en la normativa internacional mantienen hasta la actualidad una brecha de impunidad.

Como respuesta a la ciberdelincuencia de manera que se observó en la Tabla 1, los países tomaron distintas decisiones como la introducción de nuevos tipos penales, la adaptación de procedimientos penales para la persecución y sanción y el fortalecimiento de la cooperación internacional. Además, la jurisdicción universal toma lugar tras aplicar de manera explícita el principio en la normativa penal para combatir de manera efectiva la impunidad en materia de ciberdelitos. Como se ha demostrado a lo largo de la investigación la necesidad de una herramienta eficaz que sea utilizada por los Estados para sancionar a los delincuentes de ciberdelitos transnacionales a través de acuerdos internacionales.

CAPITULO II. DISEÑO METODOLÓGICO

2.1. Metodología de la investigación

La investigación científica es un elemento fundamental para el desarrollo de la sociedad porque contribuye a la generación de nuevo conocimiento que mejora la calidad de vida de las personas. Además, para Delgado (2021) promover investigación multidisciplinaria "es importante para desarrollar investigación en diferentes áreas del conocimiento y así responder a las necesidades que la sociedad nos demanda" (p. 2385). Tras comprender esto, cabe profundizar sobre el paradigma de la investigación.

Se entiende como paradigma de investigación aquel lente a través del cual el investigador entiende el fenómeno que desea estudiar. Para Finol de Franco & Vera (2020) el paradigma investigativo es "un modelo, sistema de convicción, creencias que posee el investigador en relación con el componente ontológico, axiológico, epistemológico y metodológico, lo cual conlleva a la búsqueda del camino o vía de acceso a la generación de conocimiento científico" (p. 6). En base a esto, el paradigma que escoja el investigador posee supuestos ontológicos, epistemológicos y metodológicos diferentes, y esto de manera directa influye en cómo se aborda el problema de investigación.

En la presente investigación se aborda el paradigma racional positivo, en tal sentido, es el que busca determinar un conocimiento racional y plenamente objetivo del derecho. Además, aquel es propio de la investigación jurídica debido a que su objetivo es la búsqueda de un saber que agregue nuevos conocimientos en añadidura de los existentes y aborda el derecho substantivo y procesal al estudiar la norma, la jurisprudencia y la doctrina jurídica (Becerra, 2020). En suma, el paradigma racional positivo, en el presente trabajo se presenta en la racionalización del problema de investigación donde se analiza de manera sistemática los ciberdelitos y su alcance, además de eso en base al estudio de normativas internacionales y nacionales sobre la jurisdicción en ciberdelitos.

En la misma línea, en este trabajo, el paradigma ayudó a lógicamente formular una hipótesis y luego a contrastar con la realidad en base a lo empírico y proponer una solución. Con esto se cumplió con el tercer objetivo debido a que la presente investigación se establece criterios jurídicos sobre la posibilidad de una jurisdicción universal para los ciberdelitos en la legislación ecuatoriana. En el mismo sentido, si bien es cierto que este paradigma es un fuerte pilar en la investigación jurídica, este como se observa en la presente investigación se complementa con diferentes enfoques con la finalidad de obtener una visión completa y objetiva del fenómeno jurídico.

Tras estudiar el paradigma, cabe aclarar que este y el enfoque tienen un vínculo en particular en la investigación porque a partir del paradigma antes explicado subyacen los enfoques. Para esto, Acosta (2023) expone que el enfoque es:

> La perspectiva teórica o metodológica que se utiliza para abordar un problema. Además, son los planteamientos, el punto de vista, la orientación y las formas de ver la realidad del investigador quien posee una cosmovisión que condiciona su acercamiento a la realidad que desea estudiar (p. 84).

De esta manera, los enfoques se clasifican en su mayoría en cualitativo, cuantitativo y mixto, el primero se basa en la comprensión profunda y subjetiva del fenómeno, el segundo se centra en la medición numérica de datos y estadísticas; por último, el enfoque mixto combina ambos elementos.

Tras lo mencionado y al concebir que el objeto de la investigación jurídica es la perspectiva de un mundo normativo, donde todo deriva o se fundamenta los diversos desarrollos filosóficos, doctrinarios y jurídicos (Nizama & Nizama, 2020). Es concerniente que, la ciencia social del derecho aborde y estudie fenómenos subjetivos, así la investigación descrita se sesga hacia un enfoque cualitativo. Al ser este enfoque aquel que busca además de la comprensión de los fenómenos jurídicos, el entendimiento holístico y contextualizado para la interpretación y creación de teorías.

En el mismo sentido, el enfoque cualitativo busca comprender diferentes problemas, fenómenos y situaciones sociales en base a una interpretación de datos no numéricos. En base a eso Mora (2022) menciona que el enfoque cualitativo "suele considerar técnicas tales como, por ejemplo, entrevistas abiertas, grupos de discusión, como ocurre en la antropología, técnicas relacionadas con la observación (participante y no participante), además recoge los discursos completos de los sujetos, para proceder luego a interpretarlos" (p.412). De esto se desprende que, el enfoque cualitativo es altamente flexible y adaptable, en la presente investigación por medio de técnicas como la entrevista a profesionales, además del estudio de normativa, doctrina, jurisprudencia se logró comprender el fenómeno, analizar de forma sistemática los datos receptados y determinar que la jurisdicción universal permite el procesamiento de los ciberdelitos en la legislación ecuatoriana.

Por otro lado, el tipo de investigación es la clasificación que se ejecuta en función de cada uno de los objetivos planteado, además de los métodos y técnicas manejadas en una investigación. Esta clasificación mencionada se basa en las preguntas que se buscan responder y/o los objetivos que se persiguen, de esta forma cada tipo de investigación tiene características propias y se ajusta a diferentes contextos e intenciones. En la misma línea, se verifican varios tipos como exploratorio, descriptivo, correlacional y explicativo (Álvarez-Risco, 2020).El primer tipo tiene como objetivo explorar un tema poco conocido o un desconocido fenómeno, el segundo se basa en la descripción de las características del fenómeno, el tercer tipo se centra en la relación entre dos o más variables, el último, por otro lado, recae en la explicación las causas del fenómeno.

El tipo descriptivo de la investigación tiene como objetivo el presentar una imagen clara y completa del fenómeno o situación en particular, este no busca determinar relaciones de causa y efecto. Para Guevara, Verdesoto, & Castro (2020) "se encarga de puntualizar las características de la población que está estudiando" (p.166). Tras esto las características que tiene el tipo descriptivo que se utilizó en la presente investigación es una información precisa, verídica y sistemática, además este tipo recalca las características observables y verificables, todo esto

con la finalidad de abordar el problema con mayor profundidad. En el caso del presente trabajo, el tipo descriptivo ha permitido caracterizar de manera ordenada y exacta la naturaleza de los ciberdelitos, además de relacionarla con la jurisdicción universal y de esta forma, profundizar en el fenómeno completo.

2.2. Técnicas e instrumentos de recolección de la información

Se define como método a un camino en específico que conduzca a la meta deseada. En base a esto, dentro de la metodología jurídica los métodos según Martínez (2023):

> Se dividen en dos tipologías la teórica y la empírica, en el caso de la primera permiten descubrir en el objeto de investigación, las relaciones esenciales y las cualidades fundamentales, no detectables de manera sensoperceptiva. Respecto a los segundos cuando hacemos referencia a los métodos empíricos estos se emplean en el desarrollo de procesos investigativos vinculados a la observación, experimentación, encuesta, entrevista y se fundamentan en la formulación de una hipótesis que luego se experimenta y se confirma (…) (p.2).

Tras lo explicado, la presente investigación se realizó en base a la primera tipología, es decir, se apoyó en procesos vinculados al análisis y deducción, además de cómo se observó practicar debidos procesos investigativos como la aplicación de entrevistas.

En primer lugar, el método analítico es utilizado en la investigación científica para razonar donde se separa los compendios de un todo, para posteriormente estudiarlas, establecerse relaciones y diferencias; además de conocer la verdad de un objeto o concepto complicado, que por su complicación no es estudiado de forma directa (Condori, 2021). Tras esto, en el presente trabajo, se razonó acerca de los elementos de la jurisdicción universal para su debida aplicación, además de conocer a profundidad el concepto complejo de ciberdelitos.

En base a lo mencionado, el método deductivo en investigación es un proceso de razonamiento que parte de principios generales o teorías establecidas para llegar a conclusiones específicas. Para Espinoza-Freire (2023) “se traduce esencialmente en el análisis de los principios generales de un tema específico, el que una vez comprobado, verificado y determinado, el principio es válido, de manera, que se procede a aplicarlo a contextos particulares” (p.37). De esta forma, el presente método utilizado fue un camino lógico, que al partir de lo general permitió al investigador comprender y explicar lo particular, así resolver el problema concreto.

El método dogmático, por otro lado, impulsa la sistematización del derecho gracias al planteamiento de figuras y conceptos jurídicos que eliminen lagunas y antinomias, entonces vela porque normas y conceptos se sumen al ordenamiento legal (Condori, 2021). Dentro de la presente investigación se utiliza este método al momento de reconocer ciertos vacíos en el ordenamiento legal y se plantea, a su vez, la utilización de figuras legales que dan solución al fenómeno.

En la misma línea, la modalidad de investigación fue la documental, esta tiene como objetivo guiar la investigación desde dos aspectos, uno principalmente tiene relación con información ya existente recogida de distintas fuentes; luego el investigador proporciona una visión panorámica y sistemática del fenómeno (Reyes-Ruiz & Carmona Alvarado, 2020). En el presente trabajo de manera esencialmente bibliográfica y archivística los datos fueron recopilados de libros, artículos científicos, revistas especializadas, boletines de prensa y sentencias.

Para finalizar, la técnica de investigación aplicada fue la entrevista. Como se mencionó con anterioridad esto en base al enfoque cualitativo ayudó a construir y sistematizar tablas de información recogida a una serie de personas especializadas en el tema. La entrevista está basada en tres categorías: no estructurada, semiestructurada y estructurada (Molano de la Roche, Valencia, & Apraez, 2021). Con respecto a lo mencionado, se aplicaron entrevistas estructuradas a especialistas en ciberdelitos.

Para procesar la información, en el presente trabajo de investigación se tomaron en cuenta la experiencia y los puntos de vista de profesionales en Ingeniería en Sistemas, Telecomunicaciones, Electrónicos para tener una visión completa acerca del ciberespacio y la naturaleza de los delitos cometidos en ese entorno digital. Posteriormente, se entrevistó a profesionales de Derecho Penal donde en base a su experiencia se estableció el problema sobre la persecución de ciberdelitos transfronterizos y la dinámica de la jurisdicción universal. Con base en lo referido, se determina que se lograron cumplir con los objetivos planteados en el proyecto de titulación, como se señala en los párrafos supervinientes.

Se fundamentó jurídica y doctrinariamente la jurisdicción universal y su aplicación en ciberdelitos en la legislación ecuatoriana. Esto en base a la revisión de varias fuentes académicas y distinta normativa nacional e internacional. Por consiguiente, el segundo objetivo se cumplió efectivamente debido a que se caracterizó a la jurisdicción universal en ciberdelitos en el territorio ecuatoriano, esto se dio por la correcta utilización de instrumentos para la recopilación de información detallada gracias a profesionales del tema. Por último, el tercer objetivo del presente trabajo se cumplió plenamente porque se logró establecer criterios jurídicos sobre la posibilidad de una jurisdicción universal para los ciberdelitos en la legislación ecuatoriana.

2.3. Población y muestra

En la presente investigación se realizó una muestra finita de profesionales, en base a esto no se determinó la necesidad de aplicar una fórmula de población-muestra. Con el conocimiento de ante mano que, la muestra es aquel grupo representativo que se elige de la población, esta población por otro lado es el conjunto de individuos que comparten un rasgo en común. La entrevista se realizó, por un lado, a profesionales en Ingeniería como en Telecomunicaciones, en Electrónica y en Sistemas, por otro lado, a profesionales de Derecho especialistas en Derecho Penal y/o Derecho Digital para de esa manera poder receptar información sobre la naturaleza de los ciberdelitos, ciberespacio, además de plantear la dinámica de la

jurisdicción universal. Los profesionales entrevistados se presentan en la siguiente tabla:

Tabla 5. Población y muestra

Nombre del entrevistado	Profesión	Número
Abg. Victoria Ramón	Abogada por la Universidad Nacional de Loja. Master en Criminalística por EIG Business School y Universidad Internacional del Ecuador.	**3**
Abg. Santiago Acurio	Abogado y Doctor en Jurisprudencia por la Pontificia Universidad Católica del Ecuador. Especialista en Derecho Penal por la Universidad Andina Simón Bolívar. Magister en Tecnologías para la Gestión y Práctica Docente de la Pontificia Universidad Católica del Ecuador, Magister en Derecho Digital, Transformación Digital y Economía Digital de la UDLA.	
Abg. José Moreno	Abogado por la Universidad Regional Autónoma de Los Andes. Master en Derecho mención Derecho Penal y Criminología por la Universidad Regional Autónoma de Los Andes	
Ing. Cristian Zúñiga	Ingeniero Electrónico por la Escuela Superior Politécnica de Chimborazo. Master en Evaluación y Auditoría de Sistemas Tecnológicos. Perito Informático telecomunicaciones electrónica y redes de información acreditado por el Consejo de la Judicatura.	**3**
Ing. Cristhian Cobo	Ingeniero en Sistemas por la Pontificia Universidad Católica del Ecuador. Master en Mercadeo con Mención en Mercado Digital por la Pontificia Universidad Católica del Ecuador.	
Ing. Andrés Lagua	Ingeniero en Telecomunicaciones por la Escuela Superior Politécnica de Chimborazo. Master en Seguridad Informática y Sistemas por la Pontificia Universidad Católica del Ecuador.	

Fuente: elaboración propia

CAPÍTULO III: ANÁLISIS DE LOS RESULTADOS DE LA INVESTIGACIÓN

3.1. Presentación de resultados

Tabla 6. Resultados de Abogados Penalistas

Pregunta	Abg. Victoria Ramón	Abg. Santiago Acurio	Abg. José Moreno
PREGUNTA 1 ¿De qué manera se realiza la investigación de ciberdelitos en el estado Ecuatoriano?	El ente primordial es la Fiscalía General del Estado, se encarga del tema de investigación. Actualmente, la Policía Nacional y su Unidad de Delitos Informáticos se encargan de recolección de evidencias digitales, técnicas de rastreo digitales, colaboración con proveedores de servicios, rastreo de direcciones IP, entre otros. Además, juntamente con Peritos Informáticos se realizan peritajes específicos.	La investigación en tema de ciberdelitos es parecida a la de los delitos tradicionales por cuanto el dueño de la acción penal es Fiscalía General del Estado, esta tiene Fiscalías especializadas y para este tema existe una Unidad especializada en ciberdelitos en Quito. Además, existe la Policía Cibernética. La investigación se realiza de manera pre procesal y procesal para resguardar los indicios de los delitos.	El estado ecuatoriano por medio del Código Orgánico Integral Penal, los ciberdelitos son investigados por el procedimiento ordinario como lo establece la norma indicada, se apertura una investigación previa, la Fiscalía juntamente con sus organismos auxiliares para la investigación, realiza todas las diligencias investigativas para así poder o tratar de esclarecer los hechos que presuntamente se investigan y que por medio de estos el fiscal realice una formulación de cargos.
PREGUNTA 2 ¿Qué eficacia tiene este proceso investigativo en el Ecuador?	Existen pros y contras, en primer lugar, existe visibilidad e investigación para delitos que antes no eran considerados como los delitos de pishing y hacking, existe una limitación porque la investigación se centraliza solo en ciudades como Quito y Guayaquil. En academia ya existen varias personas preparándose y se suman a los expertos con los que actualmente cuenta el país, pero así mismo existe una saturación de casos, esto forma un embudo, es decir, existe una gran taza de delitos en estos campos, pero muy poca eficiencia en la investigación. Por último, tras todo esto el país no cuenta con normativa suficiente además de que existen varias lagunas.	Si bien es cierto tenemos aún camino por recorrer si han existido ciertos avances como en la Policía Cibernética, además de que dentro de Criminalística exista la unidad de Informática Forense. Además de que cuando entre en vigor el Convenio de Cibercrimen, se tendrán muchas más herramientas que podrán ser utilizadas por el Estado para tratar ciberdelitos nacionales y transnacionales tras utilizar la Cooperación Internacional.	Si bien es cierto que es necesario mejorar en varios aspectos hay que tomar en cuenta que el proceso depende del tiempo necesario de investigación. Esto porque la investigación previa dura uno o dos años por el delito y su complejidad como una posible naturaleza transnacional, con este tiempo la fiscalía tiene la oportunidad de realizar varias diligencias investigativas, como puede ser una posible determinación del lugar de los hechos, técnicas investigativas de acuerdo con el ciberdelito cometido, de tal forma la fiscalía tendría, con mayor precisión, la posibilidad de establecer responsable.

PREGUNTA 3 ¿Cómo considera que pueden ser mejorados los procesos de investigación de ciberdelitos en Ecuador?	Se necesita fortalecer temas de infraestructura a nivel tecnológico, mejorar herramientas porque es básico democratizar los recursos en todas las ciudades del Ecuador. Es sumamente importante una constante capacitación entes como Fiscalía, Policía Nacional y Jueces. Trabajar en reformar a nivel legislativo porque como mencioné existen muchos vacíos legales en cómo tratar estos delitos, puesto que nuestro COIP es una normativa ajustada para delitos tradicionales, pero no determina acerca de los ciberdelitos entonces no da abasto a la actualidad. Por último, tomar de ejemplo normativa internacional como en la Unión Europea y poder adaptarlo al contexto del país.	Se necesita capacitación, si bien es cierto instituciones como la Policía Judicial a través de las Unidades de Cibercrimen además de Informática Forense tienen más conocimientos, todavía en otras instituciones es menester la capacitación de manera especial a Fiscales y Jueces de la Función Judicial. Tener más recursos y herramientas de informática forense, porque estas existen solo en Quito y en Guayaquil, lo que en las demás ciudades no se encuentra.	Se toma en cuenta la especialización del personal policial que labora dentro de criminalística y del Servicio Nacional de Ciencias Forenses, porque estos son los llamados a establecer por medio de sus pericias cierto grado de responsabilidad, esto quiere decir que es necesario hacer un llamado de atención al Estado para garantizar mejor grado de especialización y contar con los suficientes mecanismos tecnológicos, que lamentablemente en nuestro país carece de los mismos, además de una regulación específica para la correcta persecución y sanción.
PREGUNTA 4 ¿Es posible que el ciberdelito se perpetre en varios territorios estatales por la universalidad del ciberespacio?	Si, el ciberespacio demuestra que los delitos pueden darse a nivel mundial y tener un gran alcance. Por ejemplo, los hackers, este delito surgen en Rusia**,** pero con servidores de Estados Unidos y afecta a alguna persona en Ecuador. Esto se ha dado como el robo de información a instituciones estatales aquí en el país. Además, en estos delitos cometidos en la universalidad del ciberespacio es difícil identificar al perpetrador por el anonimato del que se benefician por el uso de las tecnologías y la ubicación real.	Si debido a que el ciberespacio es un espacio relacional donde conviven personas, tecnología e información, entonces no existe un límite territorial como en el espacio físico. En los últimos años estos delitos transnacionales han incrementado a gran escala por procesos de desarrollo tecnológico.	Al ser el mundo tecnológico tan amplio, de libre acceso y de mayor facilidad de manejo, en nuestro país ha existido varios casos que las víctimas han estado involucrados en delitos como de estafas, de apropiación de dinero por medios electrónicos, que lastimosamente al momento de las investigaciones se ha logrado establecer que sus victimarios se han encontrados en diferentes partes o países del mundo como Hong Kong, Vietnam, Singapur y muchos más, entonces queda tan vulnerable el bien jurídico protegido sobre estos delitos porque con un clic, cualquier persona comete un delito y otra lejana en material territorial ser víctima del mismo.

PREGUNTA 5 ¿Es necesaria la cooperación entre estados para llevar a cabo la investigación y juzgamiento de ciberdelitos?	Si es necesaria, en realidad el intercambio de información entre los Estados, trabajar con normativa internacional, además de desmantelar internacionalmente redes de delincuentes. Esto ayuda a una investigación en tiempo real, así de forma mancomunada se ahorran recursos y tiempo para lugar una investigación eficaz.	Si es necesaria porque en los crímenes transnacionales, se utiliza la teoría de la ubicuidad que quiere decir, que el delito es juzgado en el lugar que comenzó la acción de este o donde se consumó el delito. El Ecuador en el caso particular, el COIP se va por la teoría del resultado, el Estado sería competente cuando los resultados de estos se producen en el territorio estatal. A nivel Internacional se prefiere la teoría de la ubicuidad para la participación de los países.	Por su puesto, es tan necesaria la cooperación internacional entre todos los países del mundo porque de una u otra forma es necesario controlar este tipo de acciones, entonces si no existe una cooperación entre países no se va a poder erradicar estos delitos y peor aún van a quedar impunes.
PREGUNTA 6 ¿Cuáles son los principales desafíos para delimitar la jurisdicción en un entorno digital transfronterizo?	Existen varios inconvenientes, porque el ciberespacio no tiene limitaciones territoriales. Así esto al no estar delimitado conlleva grandes confusiones porque ejemplo, países como la Unión Europea tiene restricciones en cómo acceder a información de ese país, así otro Estado que investiga debe tener claro hasta donde que evidencias puede recolectar si el otro Estado no se lo permite.	En el caso particular, se conoce que la jurisdicción siempre tiene una connotación territorial entonces la jurisdicción se da por la Soberanía Estatal de juzgar y hacer cumplir lo juzgado; siempre y cuando se mantenga dentro de la jurisdicción de cada estado. La dificultad se da en los transnacionales cuando se necesita cooperación internacional.	Primero que exista la colaboración de todos los países, dejan de lado el pensamiento ideológico o político, segundo pues tratar de confrontar estas mafias con mano dura y establecer una similitud de sanciones entre países y tercero pues que todos los países tengan los mecanismos necesarios para afrontar esta problemática jurídica.
PREGUNTA 7 ¿Es conveniente incorporar la jurisdicción universal en la legislación ecuatoriana para garantizar la sanción de ciberdelitos en espacios transfronterizos?	Como Ecuador aún falta mucho de trabajar en el tema de ciberdelitos, como se mencionó anteriormente no existe normativa específica en este campo, y la que actualmente regula no da abasto. Si bien es cierto, delitos como pornografía infantil, terrorismo cibernético y protección de datos informativos que se alcance se ha visto que es gigante se puede planificar ya una jurisdicción universal, pero actualmente hay que trabajar en infraestructura y herramientas para la investigación, capacitación de especialistas y la cooperación internacional.	Para poder incorporar el principio de jurisdicción internacional en los ciberdelitos, considero que los delitos deben tener tal gravedad que afecte a toda la humanidad. De esta manera, los ciberdelitos al ser pluriofensivos es decir, afectar a más de un bien jurídico protegido, además de que puede existir una extrema lesividad sería un tema de debate porque internacionalmente lo que se ha tratado son temas de cooperación internacional dentro de iniciativas como el Convenio de Cibercrimen.	Claro que sí, y llegamos al mismo punto de una cooperación entre países, esto quiere decir que tengamos la misma oportunidad de sancionar a una personas de nacionalidad china como a una ecuatoriana y que la comunidad China exista esta paz social porque en otro país fue condenada la persona que cometió un ciberdelito, es así que si se implanta este tipo de jurisdicción, se comunicaría a otros países que posiblemente lo tenga y poder de mejorar este problema que hoy por hoy no se puede poner un alto.

Fuente: elaboración propia.

Análisis de preguntas

- **Pregunta 1: ¿De qué manera se realiza la investigación de ciberdelitos en el estado ecuatoriano?**

La investigación de ciberdelitos se la realiza a través de los parámetros del Código Orgánico Integral Penal, porque tienen actualmente el mismo trato de los delitos comunes prescritos en el cuerpo legal. La forma en la que se manejan todos los procesos es la denuncia, la fase preprocesal, que es cuando la Fiscalía con el apoyo de la Policía Nacional y peritos informáticos realizan varias diligencias investigativas, la formulación de cargos y la fase procesal. Al referirse de la investigación en materia de cibercrimen dentro del Ecuador, se evidencia que existe una gran necesidad de actualización no solo en el marco normativo, debido que no existe una norma específica sobre ciberdelitos, sino también de capacitación de los funcionarios encargados de las diligencias esto debido a la constante evolución y actualización de las conductas y mecanismos de la ciberdelincuencia.

- **Pregunta 2: ¿Qué eficacia tiene este proceso investigativo en el Ecuador?**

La eficacia de los procesos de investigación aún se ve afectada por diversos obstáculos, se exponen los problemas de la saturación de casos porque gracias a las nuevas tecnologías y nacientes conductas delictivas estos delitos en el país cada vez son más comunes y la cantidad de denuncias saturan el sistema, además de las constantes lagunas legales o la insuficiencia normativa en el tema de ciberdelitos que retrasan o dificultan la correcta persecución de estos. Por otro lado, la baja cantidad de recursos con los que cuenta el país para la investigación de estos hace que únicamente ciudades grandes sean quienes manejen el proceso. Si bien es cierto, para una investigación eficaz es necesario tomar en cuenta lo mencionado, también se ha visibilizado que paso a paso el país ve más importante el tema de ciberdelincuencia y se ha fortalecido su trato mediante la creación de unidades especializadas y también, la reciente adhesión el Convenio de Budapest.

- **Pregunta 3: ¿Cómo considera que pueden ser mejorados los procesos de investigación de ciberdelitos en Ecuador?**

Para mejorar los procesos de investigación de ciberdelitos primero es menester revisar y actualizar el marco legal ecuatoriano para adaptar a las nuevas modalidades de delincuencia, esto porque se visibiliza lagunas en cuanto a tipificación y sanción de ciberdelitos, esto se mejora cuando el país acoja estándares internacionales y adecue su normativa interna. Además, la capacitación continua es crucial porque, tanto policías, fiscales, peritos y jueces tengan la capacidad de respuesta frente a distintos casos así se cumple con procesos eficientes y eficaces, que no queden en impunidad. Por último, se necesita invertir en herramientas y recursos tecnológicos porque el fortalecimiento de informática forense garantiza una respuesta a la altura de delitos cada vez más complejos.

- **Pregunta 4: ¿Es posible que el ciberdelito se perpetre en varios territorios estatales por la universalidad del ciberespacio?**

Gracias a la naturaleza transfronteriza del ciberespacio se pueden cometer delitos en varios territorios estatales. Además de la comisión de ilícitos en el ciberespacio estos encuentran una vía cómoda debido a ciertos aspectos como el ocultamiento de su identidad y el anonimato esto porque todas las técnicas y herramientas disponibles en la actualidad facilitan reservar su ubicación geográfica, lo que dificulta su rastreo. Además, la falta de límites geográficos en el ciberespacio y la facilidad con la que los criminales tienen el acceso a servidores de diferentes países les permite operar no solo de manera individual sino formar redes criminales difíciles de detectar y víctimas de cualquier parte del mundo, hasta la seguridad completa de los Estados está en riesgo.

- **Pregunta 5: ¿Es necesaria la cooperación entre estados para llevar a cabo la investigación y juzgamiento de ciberdelitos?**

El cibercrimen tiene un alcance mundial es por esto por lo que es inminentemente necesaria la cooperación entre los Estados para su persecución y su sanción. La característica transfronteriza de los delitos se lo comprende como la conducta iniciada en un país puede tener consecuencias finales en otro país, así la respuesta que espere dar cada Estado aisladamente es insuficiente. La cooperación

internacional recae en aspectos como coordinación de acciones investigativas entre los países, además de recursos compartidos en dependencia de la capacidad de respuesta del Estado, y por último una respuesta coordinada esto ayuda a atrapar redes criminales que operan desde varios países.

- **Pregunta 6: ¿Cuáles son los principales desafíos para delimitar la jurisdicción en un entorno digital transfronterizo?**

La delimitación de la jurisdicción en un entorno digital transfronterizo es compleja debido a dos aspectos importantes como la naturaleza transfronteriza del ciberespacio y la falta de límites geográficos. Esto, en resumen, dificulta a los Estados parte determinar que leyes se aplican y bajo que jurisdicción se juzgará el delito. En la misma línea, cada Estado se rige bajo su propia normativa y esto dificulta la armonización para la cooperación internacional, de igual manera la velocidad a la que se desarrolla la tecnología y las conductas delictivas en este entorno causa que las leyes queden obsoletas. Por último, otro desafío recae en ubicar eficazmente a los servidores porque los perpetradores suelen utilizar distintos servidores a los de su ubicación y esto frustra las diligencias de investigación.

- **Pregunta 7**: **¿Es conveniente incorporar la jurisdicción universal en la legislación ecuatoriana para garantizar la sanción de ciberdelitos en espacios transfronterizos?**

La gravedad de las consecuencias de los ciberdelitos es global y por el mismo hecho, se necesita una respuesta global como la jurisdicción universal. Si bien es cierto, Ecuador actualmente no cuenta con capacitación e infraestructura específica para implementar de inmediato una jurisdicción universal, pero es menester fortalecerse en todos los frentes para luchar eficazmente contra el cibercrimen. Así la jurisdicción universal permite a Ecuador juzgar a los distintos autores y coautores de esta clase de delitos independientemente de donde se ha cometido el delito o su nacionalidad para proteger a todas las víctimas individuales además de la seguridad del país, garantizar la justicia y que ningún delito quede en impunidad al considerar aspectos importantes como gravedad de los delitos, eficiente cooperación internacional y salvaguardar todas las garantías procesales.

Tabla 7. Resultados de Ingenieros Electrónicos, Sistemas y Telecomunicaciones

Pregunta	Ing. Christian Zúñiga	Ing. Cristhian Cobo	Ing. Andrés Lagua
PREGUNTA 1 ¿A qué se considera ciberespacio?	Ciberespacio es el territorio digital en donde se realizan varios procesos para tratar de economizar los recursos, además de hacer más ágil las tareas que necesitamos y obtener mejores resultados.	Ciberespacio es el lugar donde se navega por medio de internet a nivel mundial.	Es el entorno digital creado para navegar a través del protocolo de comunicación global denominado Internet.
PREGUNTA 2 ¿De qué manera se delimita el territorio estatal en el ciberespacio?	Los territorios estatales se delimitan por redes de computadores, dentro de estos se evidencia como al pasar del tiempo nuevas tecnologías se adaptan como la aparición de tecnologías de internet, que esta viene a ser una red de redes. Por otro lado, se podría delimitar por direcciones IP.	Si bien se delimitan por ejemplo por redes internas o direcciones de redes locales. Pero de manera exacta no existen como físicamente los límites territoriales.	La delimitación del ciberespacio es un poco compleja por su naturaleza y entorno, porque no tiene límites como en el entorno físico. Sin embargo, se puede mencionar que aquí en el país, a través de la Ley de Protección de Datos se busca iniciar a generar una concientización y delimitación de los datos públicos y privados.
PREGUNTA 3 ¿Es posible la comisión de ilícitos en el ciberespacio y cuáles en base a su experiencia son los de mayor frecuencia?	Si se cometen delitos en el ciberespacio, pero es difícil su detección, para esto se debe tener un conocimiento amplio de lo que se conoce como informática forense, porque al igual que la investigación en el entorno físico, así también debe hacerse dentro del ciberespacio y primar el cuidado y la cadena de custodia de los indicios. Los delitos de mayor frecuencia actualmente son los fraudes financieros realizados por hackers o el robo de información de empresas por medio de malware, que luego a través de delitos como extorsión se pide más dinero por la restauración de la información.	Si se cometen delitos en el ciberespacio y en los últimos años con mayor frecuencia. Lo más común son los hackers, estos son los que cometen ciberdelitos como fishing, por ejemplo, correos falsos que envían de manera masiva, donde se abre el mismo y se infecta todo el dispositivo o toda la red de dispositivos, estos pueden desencadenar graves consecuencias. Así como infectar a dispositivos de instituciones estatales desde aquí o desde otro país y luego mediante otros delitos como la extorsión causar más daño.	Si es posible la comisión de ciberdelitos y considero que los casos más frecuentes son piratería de software, pornografía infantil, robo de información confidencial, robo de identidad, estafas y fraudes electrónicos.

PREGUNTA 4 ¿Cómo es el proceso de investigación de los ciberdelitos en el estado Ecuatoriano?	Cuando pasa un ciberdelito en el Ecuador, se tienen 2 entes a los cuales el área fiscal o los jueces acuden; estos son Policía Criminalística y Peritos Forenses. Además de la Policía Judicial en el Departamento de Ciberdelitos.	Si bien es cierto, lo que desde la ciberseguridad se trata de hacer es la prevención donde, se protege las brechas de seguridad de los dispositivos en base a ISOS y mitigar los riesgos. De ahí, una vez se sufre un ciberdelito este se reporta, además comienza el proceso de Fiscalía donde actualmente no existe una legislación específica y eficaz para los casos sucedidos en el ciberespacio.	El proceso de investigación comienza con la denuncia o la detección del individuo si es un delito flagrante, luego con la investigación técnica por DIASED, para luego pasar a la recolección de evidencia digital y el análisis forense. El proceso legal lo tiene Fiscalía, además de que cuando sea necesario re requiera cooperación internacional.
PREGUNTA 5 ¿Existe legislación internacional y/o nacional que ampara los procesos de investigación?	Es difícil que exista una normativa que resguarde eso debido a la falta de legislación especializada para ciberdelitos. Esto es un problema muy grande, porque mientras en otros países avanza a mayor velocidad la legislación, aquí en el país existen muchos vacíos, esto si llegara a instancias internacionales no se podría defender. Lo que está determinado es únicamente los delitos en el Código Orgánico Integral Penal, por otro lado, la Ley de Protección de Datos Personales y la Legislación Internacional como el Convenio de Budapest. Entonces se plantea una propuesta de ley que puede llenar todos los vacíos legales que actualmente tenemos en el tema de ciberdelitos.	De una manera específica, no existe legislación nacional para tratar la ciberdelincuencia, existe desconocimiento desde las autoridades para investigar de manera efectiva y luego sancionar. Lo que se regresa a ver es la normativa internacional.	Ecuador cuenta con legislación que sin ser específica se habla sobre los ciberdelitos como el Código Orgánico Integral Penal (COIP), Ley de Comercio Electrónico, Firmas y Mensajes de Datos. Como mencioné si hablan sobre estos, pero no son precisos con la regularización de los procesos de investigación y la jurisdicción. Por otro lado, de manera internacional está el Convenio de Budapest sobre Ciberdelincuencia, además de la Convención de las Naciones Unidas contra la Delincuencia Organizada y algunos Convenios INTERPOL.

Fuente: elaboración propia.

Análisis de preguntas:

- **Pregunta 1**: **¿A qué se considera ciberespacio?**

Se considera que el ciberespacio es aquel universo digital que se encuentra interconectado, además la manera de acceder a este es a través del uso del internet. Al ser el ciberespacio un entorno dinámico y constante, se determina que a nivel global dentro de este se realizan cientos de actividades como la comunicación, almacenamiento, interacción e intercambio de información.

- **Pregunta 2: ¿De qué manera se delimita el territorio estatal en el ciberespacio?**

El desafío de delimitar el territorio de cada estado en el ciberespacio es complejo y multifacético debido a que no solo se consideran aspectos técnicos sino también dimensiones legales y políticas. Así para de delimitar el territorio estatal en el ciberespacio, se considera que la naturaleza del internet es global y, por ende, descentralizada, esto no permite que existan límites en fronteras claros. Además, que las direcciones IP que actualmente sirven para ubicar las acciones dentro del ciberespacio son un indicador, pero no siempre determinan una ubicación física exacta. Por otro lado, para la delimitación del territorio también se consideran aspectos legales y políticos porque actualmente se han realizo esfuerzos para lograrlo de manera precisa pero la velocidad a la que evoluciona la tecnología y la naturaleza transfronteriza de Internet hacen que la normativa resulte desactualizada o insuficiente.

- **Pregunta 3: ¿Es posible la comisión de ilícitos en el ciberespacio y cuáles en base a su experiencia son los de mayor frecuencia?**

Dentro del ciberespacio es común la comisión de delitos o actividades ilícitas, esto como resultado de la naturaleza global y anónima del internet, además de conocimientos y experiencia en tecnologías. En la misma línea gracias a la evolución constante de las tecnologías los delitos se adaptan a las tendencias y la

universalidad del ciberespacio dificulta la persecución de estos. Dentro de los delitos más frecuentes se encuentran, phishing, ransomware, robo de identidad, estafa en línea, piratería informática, acceso no autorizado a sistemas informáticos, malware, pornografía infantil, ciberacoso.

- **Pregunta 4: ¿Cómo es el proceso de investigación de los ciberdelitos en el estado ecuatoriano?**

Para realizar el proceso de investigación de ciberdelitos actualmente se lo hace de manera similar a la de los delitos tradicionales con ciertas variables. Primero se da paso a la denuncia formal en Fiscalía, posteriormente entes como la Policía Nacional, a través de unidades especializadas inicia la investigación previa para recopilar información. Luego de esto, se procede a la recolección y análisis de evidencia digital por parte de especialistas se tienen en cuenta protocolos forenses para garantizar la integridad. En base a eso, se desarrolla la investigación criminal, que incluye ya sospechosos. Así se presenta cargos y el caso pasa a la fase judicial para que se dicte sentencia.

- **Pregunta 5: ¿Existe legislación internacional y/o nacional que ampara los procesos de investigación?**

En el marco normativo ecuatoriano si bien existen algunos instrumentos legales que determinan varios aspectos relacionados con la investigación y sanción de los Ciberdelitos, como el Código Orgánico Integral Penal (COIP), pero este aún tiene lagunas y varios desafíos. De esto deriva que, en el Ecuador, es inminente la falta de especificidad en el tratamiento de ciberdelitos como en la investigación en aquellos que son transfronterizos y la necesidad de cooperación internacional. Por otro lado, la veloz evolución de las tecnologías y las nuevas particularidades de ciberdelitos dificultan la tarea de mantener la legislación actualizada. Por último, en estos procesos, existe una falta de capacitación especializada en ciber investigación entre los operadores de justicia.

3.2. Análisis general de resultados

Tras la utilización de los instrumentos para la recopilación de información como la aplicación de entrevistas estructuradas a profesionales y cumplir lo estipulado en la metodología, se analiza de manera general los resultados obtenidos. Se busca sinterizar los principales hallazgos de la investigación, en relación con la hipótesis planteada que la jurisdicción universal permite el procesamiento de los ciberdelitos en la legislación ecuatoriana.

Para empezar, se toma en cuenta que tanto especialistas en distintos campos como la Ingeniería y el Derecho concuerdan en la novedad del ciberespacio. Este es el entorno digital interconectado donde se llevan a cabo cientos de actividades, desde una simple comunicación interpersonal hasta complejas transacciones económicas o el almacenamiento de información crucial de un Estado. En base a esto técnicamente, se ha corroborado que el entorno cibernético al ser un vasto océano de información conectada por internet no tiene límites territoriales, es decir, cualquier computadora o dispositivo tecnológico conectado a internet desde cualquier parte del mundo entra al espacio digital sin limitación de fronteras, océanos o continentes.

Tras esto, surgen distintas problemáticas en el ciberespacio, una de estas es la ciberdelincuencia. Después de la explicación de los expertos es bastante común la comisión de delitos en este entorno. La ciberdelincuencia se la entiende como aquellas actividades ilícitas cometidas en el espacio cibernético por medio del uso de la tecnología. Aquella genera billones de dólares de ingresos anualmente, como se evidenció en la presente investigación es la tercera economía más grande del mundo.

De esta manera, la naturaleza transfronteriza del ciberespacio asegura de cierta manera la impunidad de los perpetradores por su difícil persecución. En ese sentido, organismos internacionales como la Interpol y la Europol comunican que la verdadera complejidad de una investigación cuando se dan ciberdelitos transnacionales se da por factores como la multiplicidad de jurisdicciones y la

inexactitud de cooperación internacional. Además de esto, aspectos del ciberespacio como el anonimato web, la habilidad de acceso a servidores de diferentes países, la fácil comisión de ilícitos en cualquier parte del mundo y la búsqueda de víctimas de otros Estados, transforman el alcance de la problemática a uno mundial.

En la misma línea, el hecho de delimitar una jurisdicción en un entorno digital transfronterizo es complejo debido a que no existen límites evidentes y que la jurisdicción penal se basa mayormente en el principio de territorialidad. Este principio diseñado para el mundo físico encuentra dificultad para adaptarse al ciberespacio, porque establece que un país tiene jurisdicción para juzgar aquellos ilícitos cometidos dentro de su territorio. En el entorno digital es complejo determinar realmente donde ocurre el delito, por ende, en base a la doctrina se determina la necesidad de observar el principio de ubicuidad que se aplica cuando la conducta se haya posiblemente desarrollado en otro lugar, pero los efectos se dan en el territorio nacional. En relación con lo mencionado, la normativa que actualmente regula la investigación y sanción de estos delitos tiene varias lagunas, vacíos y falta de actualización en los procesos.

La normativa ecuatoriana en cuanto a la investigación y sanción de ciberdelitos encuentra los lineamientos en Código Orgánico Integral Penal (COIP), al aplicar procesos similares a los delitos comunes. El proceso de investigación como se explica por parte de los expertos y una investigación normativa nacional comienza por la denuncia, la fase preprocesal, la formulación de cargos y la etapa procesal. Dentro de la investigación, el momento donde interactúan distintos organismos como Fiscalía, Policía y Peritos Especializados, el sistema enfrenta limitaciones significativas como una normativa desactualizada que no cumple con los estándares internacionales, además la falta de capacitación de los operadores de justicia ante la creciente complejidad de ciberdelincuencia.

En base al principio de seguridad jurídica establecido en la Constitución de la República del Ecuador, y al considerar la ratificación del Convenio de Budapest en el país la normativa interna se adapta a los estándares internacionales. Bajo esa

premisa, el Estado encuentra el momento oportuno no solo de regular los ciberdelitos en la normativa nacional, sino plantear la jurisdicción universal para su procesamiento efectivo en base a la propuesta presentada a continuación:

Tabla 8. Criterios Jurídicos Jurisdicción Universal en Ciberdelitos en la Legislación Ecuatoriana

Criterio		Elementos/Análisis
Multiplicidad de Jurisdicciones	**Transnacionalidad**	Por el carácter transnacional del ciberespacio la delimitación de la jurisdicción es compleja. Cuando el lugar de cometimiento es distinto al lugar de la víctima o el lugar de los servidores, la jurisdicción universal permitirá al Estado juzgar al perpetrador independientemente del lugar de comisión del delito o su nacionalidad.
	Legislación Convergente	Al convivir varias jurisdicciones estatales, se encuentran distintas legislaciones que al no tener una normativa común acerca de la investigación y sanción de los ilícitos o un acuerdo sobre la jurisdicción se generan conflictos. La jurisdicción universal al ser un principio jurídico conocido a nivel mundial y aplicable resulta una solución común.
Gravedad de Ciberdelitos	**Afectación global**	Las redes digitales conectan a todo el mundo en tiempo real esto genera un alcance inimaginable de ciberataques. De esta forma desde el bienestar individual hasta la infraestructura de los Estados y sus instituciones de energía, salud, comunicaciones son afectados. Además, se genera pérdidas económicas de billones de dólares y es una gran amenaza a la Seguridad Nacional de los países. Bajo esta premisa, la jurisdicción universal al establecerse como un mecanismo de respuesta a crímenes graves de alcance mundial es la vía efectiva.
	Pluralidad de bienes jurídicos protegidos	Existe una amplia variedad de derechos afectados por la ciberdelincuencia. Las consecuencias de esta problemática alcanzan a múltiples víctimas, afectan una amplia gama de bienes protegidos desde la privacidad, la integridad física, la propiedad y la seguridad nacional. Además, los efectos suelen ser en cascada, es decir, tras el cometimiento de un ciberdelito se desencadenan varios efectos negativos. El carácter pluriofensivo y la violación de derechos humanos fundamentales a gran escala de la ciberdelincuencia justifica que la respuesta internacional sea la jurisdicción universal.

Rápida Evolución de Conductas	**Riesgo de leyes obsoletas**	La tecnología y sus herramientas se desarrollan a un ritmo vertiginoso así los ciberdelitos cada vez son más sofisticados e indetectables. En la misma línea, los marcos legales son más lentos en adaptarse a la realidad que supone una era digital y el riesgo de esto son los vacíos legales que no son resueltos hasta poder realizar otro mecanismo de combate. Este desface de tiempo lo aprovechan los ciberdelincuentes para no ser sancionados. De esta manera, aunque las leyes queden obsoletas los principios como la jurisdicción universal son útiles y la interpretación de la normativa nacional se considera flexible.
	Prevención	Bajo la rápida evolución de los ciberdelitos la cultura de la prevención es una opción viable. De esta manera, con la actualización de ciberseguridad y la herramienta segura de la jurisdicción universal se prevé el desarrollo de nuevas tecnologías y conductas delictivas cada vez menos detectables.
Cooperación Internacional	**Optimización de recursos y herramientas para la prosecución procesal**	Los Estados con mejores recursos permiten procesar de manera más eficiente los ciberdelitos, además al estandarizar las herramientas se insta a la creación de unidades especializadas, bases de datos compartidas y el intercambio de prácticas entre profesionales. De esta manera, la jurisdicción universal además de optimizar la respuesta de los Estados crea un ambiente propicio para la intercomunicación y desarrollo profesional durante la investigación y sanción de ciberdelitos.
	Instrumentos Internacionales	Al conferir legitimidad y aceptación a la jurisdicción universal los instrumentos internacionales que se creen son los que establecen normas comunes no solo de los elementos constitutivos de los ciberdelitos sino también de mecanismos efectivos de asistencia mutua para evitar la fragmentación del derecho internacional.
Fortalecimiento Interno	**Reforma al COIP**	La tipificación clara de los ciberdelitos tras adaptar al COIP a los estándares internacionales es parte del fortalecimiento interno, además de ser el momento oportuno para añadir la jurisdicción universal en la norma mediante una reforma. De esta manera, la justicia ecuatoriana conocerá estos delitos así sean cometidos en el extranjero porque afectaron intereses de los ecuatorianos, cuando el responsable esté en el país o mediante la utilización de sus servidores.
	Creación de reglamentos	Para la investigación y juzgamiento es necesario elaborar reglamentos claros y específicos con la finalidad de poner en marcha la jurisdicción universal. En la misma línea, velar por los derechos de las víctimas y asegurar la protección de pruebas digitales. Todo esto también garantiza y facilita la cooperación internacional.

	Capacitación especializada	Todos los operadores de justicia como Fiscalía, Policía y Jueces al capacitarse de manera técnico-jurídica sobre los ciberdelitos y comprender la complejidad de los delitos garantizan la correcta aplicación de la justicia, además de fomentar un espacio de intercambio de conocimientos y herramientas al cooperar internacionalmente.

Fuente: elaboración propia

CONCLUSIONES

- Existe la necesidad de aplicar la jurisdicción universal en delitos cibernéticos, debido a que, ésta es una herramienta eficaz que se ha utilizado a lo largo de la historia para combatir la impunidad, además responde de manera efectiva a la investigación y sanción de ciberdelitos que por su característica transfronteriza es compleja la delimitación de la jurisdicción Estatal, de tal manera que conviene priorizar la cooperación internacional y el vigoroso procesamiento de los delitos.

- En el capítulo 1 del presente trabajo, se fundamentó jurídica y doctrinariamente la jurisdicción universal, de esta manera se concluye que su aplicación en la historia ha funcionado para combatir la impunidad en delitos complejos y graves que afecten a varios bienes jurídicos de la población global, además en el Ecuador está reconocida en su normativa constitucional y penal con enfoque en delitos de lesa humanidad, pero debido a la veloz evolución de la humanidad y su constante interacción con la tecnología el alcance de esta jurisdicción se ha ampliado. Por ende, es viable aplicación en ciberdelitos, por factores como su naturaleza transfronteriza, la complejidad de la investigación y la multiplicidad de jurisdicciones para procesarlos.

- La jurisdicción universal permite a los Estados juzgar y sancionar al perpetrador de delitos graves independientemente del lugar donde se cometió el crimen, debido a que esta es extraterritorial y complementaria. En el país, por un lado, de manera técnico-legal, procesos investigativos y sancionatorios de ciberdelitos carecen de una regulación actualizada acorde a la realidad de la sociedad y una eficacia veraz porque los delitos cibernéticos permanecen en una tasa alta de impunidad. Además, de manera técnica, por la falta de barreras geográficas, aspectos transfronterizos, utilización fraudulenta de servidores y anonimato en el ciberespacio es complejo delimitar la jurisdicción de cada Estado, por lo que

es necesariamente alarmante la aplicación de la cooperación internacional para combatir la ciberdelincuencia a través de la jurisdicción universal.

- Los criterios jurídicos para aplicar la jurisdicción universal en ciberdelitos son 1. Naturaleza Transnacional del ciberespacio 2. Legislación Convergente 3. Afectación global de la ciberdelincuencia 4. Pluralidad de bienes jurídicos protegidos 5. Riesgo de leyes obsoletas 6. Prevención frente a nuevas modalidades 7. Optimización de recursos y herramientas para la prosecución procesal 8. Instrumentos Internacionales 9. Reforma al Código Orgánico Integral Penal 10. Creación de reglamentos internos 11. Capacitación especializada, con lo que se ayudaría a combatir estos delitos y evitar su impunidad.

RECOMENDACIONES

- En base a los resultados metodológicos sobre la creciente vulnerabilidad del país ante ciberataques y la posición de blanco fácil que tiene el Ecuador frente a la ciberdelincuencia mundial, se recomienda que a las autoridades ecuatorianas a priorizar la ciberseguridad como un asunto de seguridad nacional. En la misma línea, se insta a fortalecer la capacitación de profesionales en ciberseguridad, incrementar la inversión en tecnología de seguridad y crear concientización en la sociedad sobre la transcendencia del ciberespacio.

- A partir del análisis de los resultados del trabajo, se recomienda a la Asamblea General del Ecuador que analice a profundidad el proceso de adhesión de convenios e instrumentos internacionales en materia penal. Esto por cuanto, es alarmante que, a pesar de la ratificación de numerosos acuerdos internacionales, existen brechas importantes entre la normativa interna y los compromisos adquiridos a nivel internacional. Así se insta a este órgano legislativo que realice un estudio a detalle de los instrumentos ratificados y velar por la actualización y adaptación de la legislación nacional al elaborar nuevas leyes, asignación de recursos y mecanismos de seguimiento. Para que la sociedad goce de los beneficios concretos de los instrumentos internacionales.

- Se recomienda a las autoridades del Ecuador, tras concluir la presente investigación y en referencia al punto de vista de expertos, fortalecer e invertir de manera estratégica en infraestructura a nivel tecnológico investigativo de ciberdelitos, además se insta a democratizar estos recursos en todas las ciudades del Ecuador. Con esto, se empodera a todas las entidades del país a responder de manera efectiva a las amenazas cibernéticas y nivelar el campo de juego en zonas urbanas y rurales.

- A través de la guía de expertos, se recomienda a las instituciones estatales encargadas de la recopilación de datos como Instituto Nacional de

Estadística y Censos (INEC), Ministerio del Interior, Consejo de la Judicatura, Fiscalía General del Estado implementen un sistema de recolección y análisis de datos más robusto y actualizado. Solo de esta manera con una coordinación interinstitucional, en el tema penal permite a las autoridades pertinentes tomar decisiones basadas en evidencia, identificar patrones criminales y con el objetivo de combatir la delincuencia y la seguridad del Estado, diseñar marcos normativos más eficientes.

BIBLIOFRAFÍA

Acosta, S. (2023). Los enfoques de investigación en las Ciencias Sociales. *Revista Latinoamericana Ogmios*, 82-95.

Acurio del Pino, S. (2016). Delitos informáticos: generalidades. Universidad de Guadalajara.

Álvarez-Risco, A. (2020). Clasificación de las investigaciones. *Universidad de Lima*, 5-10.

Arrazola, A. (2019). Conflictos de jurisdicción en materia de ciberdelitos: problemática y soluciones. Madrid, España: Universidad Rey Juan Carlos.

Baltán, L. (2022). Un acercamiento a la jurisdicción constitucional como principio legitimador de la democracia sustancial. *Encuentros. Revista de Ciencias Humanas, Teoría Social y Pensamiento Crítico.*, 384-410.

Barrios, G., & Marquéz, J. (2024). Regulación de los Ciberdelitos en El Convenio de Budapest: Aspectos Normativos y Desafíos de Cooperación Internacional a partir de la Comparación entre Colombia Y Alemania. In C. Montalvo, J. Zuluaga, & L. Astrain, *Desafíos actuales del Derecho penal y la Política criminal en Alemania y Latinoamérica* (p. 623). Würzburg: ECKHAUS VERLAG.

Bartolomé, M., & Monteiro, A. (2021). El ciberespacio, durante y después de la pandemia COVID-19. *Revista De La Academia Del Guerra Del Ejército Ecuatoriano*.

BBC News Mundo. (2019, Abril 12). *Julian Assange: así fue la gran filtración de documentos clasificados en 2010 por la que EE.UU. pide la extradición del fundador de WikiLeaks.*

Becerra, K. (2020). Investigación cualitativa crítica y derecho: Análisis de su rol en la academia chilena y un estudio de caso. *Revista Pedagogía universitaria y didáctica del Derecho*, 149-176.

Becker, S., & Viollier, P. (2020). La implementación del Convenio de Budapest en Chile: un análisis a propósito del proyecto legislativo que modifica la Ley 19.223. *Revista de derecho (Concepción)*, 75-112.

Castillo, M. (2024). Investigación de ciberdelitos como medio de tutela judicial efectiva. Ambato, Ecuador: Universidad Católica del Ecuador. Sede Ambato.

Center For Strategic & International Studies. (2024, Noviembre). *Incidentes cibernéticos significativos.*

Código Orgánico Integral Penal [COIP]. (2024). Registro Oficial. Ecuador.

Condori, G. (2021). Metodología de la investigación jurídica y el impacto científico de las tesis de maestría en derecho de una escuela de posgrado de Tacna, periodo 2017-2019. Universidad Privada de Tacna.

Consejo de Europa. (2001). Convenio sobre la ciberdelincuencia. Budapest: Consejo de Europa.

Constitución de la República del Ecuador [CRE]. (2008). Registro Oficial 449 de 20 de octubre de 2008.

Cornejo, J. (2021). Criminalidad informática y la discusión sobre el bien jurídico protegido en los delitos informáticos. In P. U. Perú.

Corozo, E. (2024). Implicaciones y desafíos del ciberespacio para la aplicación del Derecho Internacional. *Revista Política Internacional*, 219-233.

Cueva, S., & Tapia, F. (2022). Niños, niñas y adolescentes en las redes sociales: estudio sobre los sistemas de protección y prevención judicial. Guayaquil: ULVR Facultad de Ciencias Sociales y Derecho Carrera de Derecho.

Cybersecurity Ventures. (2024, Junio 24). *Cybercrime Magazine.*

Defensoría del Pueblo de Perú. (2023, Mayo). *Informe Defensorial N° 001-2023-DP/ADHPD.*

Delgado, J. (2021). La investigación científica: su importancia en la formación de investigadores. *Ciencia Latina Revista Científica Multidisciplinar*, 2385-2386.

EMB Ciberseguridad Chile. (2024, enero). *Ciberseguridad en Chile: estadísticas, desafíos, tecnologías y más.*

Erique-Zambrano, A. (2022). La obligación de prevenir sancionar y castigar las graves violaciones al Derecho Internacional Humanitario en ejercicio de la jurisdicción universal en el Ecuador. *593 Digital Publisher CEIT*, 611-624.

Escriche, J. (1869). *Diccionario razonado de legislación y jurisprudencia.* España: Librería de Garnier (Paris).

Espinoza-Freire, E. (2023). La enseñanza de las ciencias sociales mediante el método deductivo. *Revista Mexicana de Investigación e Intervención Educativa*, 34-41.

Finol de Franco, M., & Vera, J. (2020). Paradigmas, enfoques y métodos de investigación: análisis teórico. *Mundo recursivo*, 1-24.

Fiscalía General del Estado. (2024, Septiembre). *Operación KAERB: red criminal internacional dedicada a delitos cibernéticos es desarticulada con la participación de fiscalías y policías de 6 países.*

Fiscalía General del Estado (2021). Perfil Criminológico Ciberdelitos. *Revista Científica de Ciencias Jurídicas, Criminología y Seguridad*, 6-62.

Gil, A. (2023). La ciberseguridad en la Seguridad Nacional: amenazas y retos en el ciberespacio. *Revista de Inteligencia y Seguridad*, 61-93.

Guevara, G., Verdesoto, A., & Castro, N. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). *Recimundo*, 163-173.

Guzmán, C., Palacios, D., & Palacios, E. (2023). Incidencias de los ciberdelitos y sus regulaciones en la ciudad de Panamá. *Revista Semilla Científica* , 524-539.

Hertler, F. (2024). Ciberdelitos 2024: El Convenio de Budapest y su influencia en el derecho penal argentino. *Nueva Crítica Penal*, 16-59.

Höffler, K., & Sommerer, L. (2021). Interconnected Society Interconnected (Criminal) Law. In EuCLR, *European Criminal Law Review* (pp. 320 - 342). Nomos.

Interpol. (2021). *La ciberdelincuencia traspasa fronteras y evoluciona a gran velocidad.*

Martínez, I. (2023). Sobre los métodos de la investigación jurídica. *Revista Chilena de Derecho y Ciencia Política*, 1-4.

Martins, B. (2022). Convenio de Budapest sobre la Ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México. *Derechos Digitales América*.

Mejía, M., Hurtado, S., & Grisales, A. (2023). Ley de delitos informáticos colombiana, el convenio de Budapest y otras legislaciones. *Revista de ciencias sociales*, 356-372.

Ministerio del Interior Ecuador . (2023, Abril 11). *Expertos en seguridad expondrán estrategias y acciones para combatir la ciberdelincuencia.*

Molano de la Roche, M., Valencia, A., & Apraez, M. (2021). Características e importancia de la metodología cualitativa en la investigación científica. *Revista Semillas del Saber*, 18-27.

Mora, R. (2022). El valor de la investigación cualitativa y la comprensión: Un examen crítico. *Educare*, 410-426.

Nizama, M., & Nizama, L. (2020). El enfoque cualitativo en la investigación jurídica, proyecto de investigación cualitativa y seminario de tesis. *Vox juris*, 69-90.

Ochoa, A. (2021). Desafíos globales del cibercrimen: caso Ecuador período 2014–2019. Quito, Ecuador: Universidad Andina Simón Bolívar.

Pastorini, J. (2020). Prevención y persecución de Ciberdelitos: ¿Un nuevo terreno para la Inteligencia Artificial? *RIDP Libri*, 92-99.

Payer, A. (2024). El principio de territorialidad y la participación delictiva transnacional. *Revista Penal*, 203-222.

Pino, E., Rojas, J., & Copa, D. (2021). La Jurisdicción Universal. Una novel figura en la legislación penal ecuatoriana. *Dilemas contemporáneos: educación, política y valores*.

Policía de Investigaciones de Chile. (2022, abril). *Ciberdelitos continuaron al alza en 2021.*

Poó-Figueroa, X. (2024). A 25 años del Caso Pinochet: testigo y parte. *Revista Comunicación y Medios*, 61-67.

Quezada, P., Suarez, E., Coloma, A., Ruiz, R., Pinos, B., Espinoza, E., . . . Martínez, C. (2022). Sobreexposición de adolescentes a Ciberdelitos en el Ecuador. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 419-435.

Resolución No. 0152-07-HC (Corte Constitucional del Ecuador Julio 26, 2007).

Reyes-Ruiz, L., & Carmona Alvarado, F. (2020). La investigación documental para la comprensión ontológica del objeto de estudio. Universidad Simón Bolivar.

Rodriguez, P., & Méndez, L. (2023). La Corte Penal Internacional en el derecho penal mexicano frente al principio de jurisdicción universal. *Ciencia y Mar*, 31-38.

Saltos, M., Robalino, J., & Pazmiño, L. (2021). Análisis conceptual del delito informático en Ecuador. *Conrado*, 343-351.

Tanque de Análisis y Creatividad de las TIC (TicTac). (2023, abril). *Estudio anual de Ciberseguridad 2022-2023.*

Tapia, L. (2022). Tecnología y derecho: una mirada al comercio electrónico, el cibercrimen y el soft law. *Ars Iuris Salmanticensis*, 199-226.

Valencia, E. (2024). Aplicación del Derecho Internacional en el Ciberespacio. *Cuadernos de Nuestra América*, 31-42.

Vinelli, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Ius Et Praxis*, 95-110.

ANEXOS

Anexo 1. Entrevista Estructurada – Abogados especialistas en Derecho Penal y Derecho Digital

- Pregunta 1: **¿De qué manera se realiza la investigación de ciberdelitos en el estado ecuatoriano?**
- Pregunta 2: **¿Qué eficacia tiene este proceso investigativo en el Ecuador?**
- Pregunta 3: **¿Cómo considera que pueden ser mejorados los procesos de investigación de ciberdelitos en Ecuador?**
- Pregunta 4: **¿Es posible que el ciberdelito se perpetre en varios territorios estatales por la universalidad del ciberespacio?**
- Pregunta 5: **¿Es necesaria la cooperación entre estados para llevar a cabo la investigación y juzgamiento de ciberdelitos?**
- Pregunta 6: **¿Cuáles son los principales desafíos para delimitar la jurisdicción en un entorno digital transfronterizo?**
- Pregunta 7: **¿Es conveniente incorporar la jurisdicción universal en la legislación ecuatoriana para garantizar la sanción de ciberdelitos en espacios transfronterizos?**

Entrevista Estructurada – Ingenieros especialistas en Sistemas, Telecomunicaciones y Electrónico

- Pregunta 1: **¿A qué se considera ciberespacio?**
- Pregunta 2: **¿De qué manera se delimita el territorio estatal en el ciberespacio?**
- Pregunta 3: **¿Es posible la comisión de ilícitos en el ciberespacio y cuáles en base a su experiencia son los de mayor frecuencia?**
- Pregunta 4: **¿Cómo es el proceso de investigación de los ciberdelitos en el estado ecuatoriano?**
- Pregunta 5: **¿Existe legislación internacional y/o nacional que ampara los procesos de investigación?**