UNIVERSIDAD TECNOLÓGICA ECOTEC

FACULTAD:

DERECHO Y GOBERNABILIDAD

TÍTULO:

“AGENTE ENCUBIERTO INFORMÁTICO SU VIABILIDAD EN EL PROCESO PENAL ECUATORIANO”

LÍNEA DE INVESTIGACIÓN

GESTIÓN DE LAS RELACIONES JURÍDICAS

MODALIDAD DE TITULACIÓN:

PROYECTO DE INVESTIGACIÓN

CARRERA:

DERECHO

TÍTULO A OBTENER:

ABOGADO

AUTOR:

ARIANNA FERNANDA PAZMIÑO TORRES

TUTOR:

MGTR. ROGER NIETO MARIDUEÑA

GUAYAQUIL, ECUADOR 2023

DEDICATORIA

A Dios, mis papás, mis abuelos y mis hermanos.

AGRADECIMIENTO

En primer lugar, quiero agradecer a Dios por ser mi guía y fortaleza para enfrentar cada paso que doy en la vida.

A Roberto y Gina, mis padres, que son mi ejemplo e inspiración, gracias por enseñarme a ser perseverante y paciente, con gran esfuerzo me han dado la oportunidad de estudiar y llegar hasta donde estoy, cada logro de mi vida se lo debo a ustedes.

A mis abuelos que son un pilar fundamental en mi vida; a mi abuelita Nancy, por estar siempre conmigo apoyándome y velando por mi bienestar.

A mi papá Raúl, que desde el cielo me cuida y celebra cada logro, su apoyo incondicional fue fundamental para que pudiera lograr mis sueños, este logro va especialmente dedicado a ti.

A mis hermanos, son la razón de sentirme tan orgullosa de culminar mi carrera.Y por último a toda mi familia y amigos, gracias por ser parte de mi vida y por celebrar este logro junto a mí.

CERTIFICADO DE REVISIÓN FINAL

ANEXO N°15

CERTIFICADO DEL PORCENTAJE DE COINCIDENCIAS

Habiendo sido nombrado Roger Nieto Maridueña, tutor del trabajo de titulación **Agente encubierto informático su viabilidad en el derecho penal ecuatoriano**, elaborado por **Arianna Fernanda Pazmiño Torres**, con mi respectiva supervisión como requerimiento parcial para la obtención del título de Abogado.

Se informa que el mismo ha resultado tener un porcentaje de coincidencias 4% mismo que se puede verificar en el siguiente link: https://app.compilatio.net/v5/report/46365303f30a0058fd76d10b36d1a0e5508b670c/sources

Adicional se adjunta print de pantalla de dicho resultado.

ROGER NIETO MARIDUEÑA

FIRMA DEL TUTOR
Mgtr. Roger Nieto Maridueña

ANEXO N°16

CERTIFICADO DE APROBACIÓN DEL TUTOR PARA LA PRESENTACIÓN DEL TRABAJO DE TITULACIÓN CON INCORPORACIÓN DE LAS OBSERVACIONES DE LOS MIEMBROS DEL TRIBUNAL

Samborondón, 10 de agosto de 2023

Magíster
Andres Madero Poveda
Decano de la Facultad
Derecho y Gobernabilidad
Universidad Tecnológica ECOTEC

De mis consideraciones:

Por medio de la presente comunico a usted que el trabajo de titulación TITULADO: **AGENTE ENCUBIERTO INFORMÁTICO SU VIABILIDAD EN EL PROCESO PENAL ECUATORIANO**, según su modalidad PROYECTO DE INVESTIGACIÓN; fue revisado y se deja constancia que el estudiante acogió e incorporó todas las observaciones realizadas por los miembros del tribunal de sustentación por lo que se autoriza a **Pazmiño Torres Arianna Fernanda,** para que proceda a la presentación del trabajo de titulación para la revisión de los miembros del tribunal de sustentación y posterior sustentación.

ATENTAMENTE,

ROGER HECTOR NIETO MARIDUEÑA

Mgtr. Roger Nieto Maridueña

Tutor

RESUMEN

El agente encubierto informático es una figura innovadora en el marco legal ecuatoriano, que se ha propuesto para hacer frente a los desafíos que presenta el cibercrimen. Este agente opera en el espacio virtual, recopilando evidencia e información de manera encubierta, lo que permite a las autoridades investigar y proceder contra los actos delictivos en línea. Utilizando una metodología de tipo cualitativa ya que se desarrollaron entrevistas a expertos en seguridad y a jueces de lo penal, estableciendo como resultado que la Ley para la Aplicación del Agente Encubierto Informático ofrece un modelo operativo para este tipo de investigaciones. Define los criterios y condiciones bajo los cuales se puede emplear un agente encubierto, limitándose a ciertos delitos graves y requiriendo justificación de su uso. Sin embargo, el rol que cumple el agente encubierto informático presenta varios vacíos legales dentro de la legislación ecuatoriana, en consecuencia, es crucial realizar una revisión detallada sobre su viabilidad, alcance y temporalidad dentro de las facultades asignadas. En cuanto a su validez en el proceso penal ecuatoriano, la Ley para la Aplicación del Agente Encubierto Informático debe ser ajustada a los principios fundamentales del sistema de justicia ecuatoriano, proporcionando las garantías necesarias para el debido proceso. Con la finalidad de respetar los derechos y libertades de los ciudadanos para garantizar su relevancia y eficacia en respuesta a los desarrollos tecnológicos y las tendencias emergentes del cibercrimen.

Palabras claves: Agente Encubierto Informático, Legislación Ecuatoriana, Cibercrimen, Investigación Digital, Principios Fundamentales

ABSTRACT

The computer undercover agent is an innovative figure in the Ecuadorian legal framework, which has been proposed to face the challenges presented by cybercrime. This agent operates in virtual space, covertly collecting evidence and information, allowing authorities to investigate and prosecute online criminal acts. Using a non-experimental, qualitative methodology since interviews with security experts were developed, establishing as a result that the Law for the Application of the Computer Undercover Agent offers an operational model for this type of investigation. Defines the criteria and conditions under which an undercover agent can be used, limited to certain serious crimes and requiring justification for their use. The role that the undercover agent fulfills presents several legal gaps within Ecuadorian legislation, consequently, it is crucial to carry out a detailed review of its feasibility, scope and temporality within the assigned Powers. Regarding its validity in the Ecuadorian criminal process, the Law for the Application of the Computer Undercover Agent conforms to the fundamental principles of the Ecuadorian justice system, providing the necessary guarantees for due process. In order to respect the rights and freedoms of citizens to ensure their relevance and effectiveness in response to technological developments and emerging trends in cybercrime.

Keywords: Computer Undercover Agent, Ecuadorian Legislation, Cybercrime, Digital Investigation, Fundamental Rights

Índice de contenidos

Introducción

Antecedentes

A lo largo de la historia, el avance tecnológico ha generado nuevos desafíos para el sistema legal y la persecución de los delitos. Con la creciente expansión de las actividades delictivas en el ámbito digital, ha surgido la necesidad y la urgencia de adaptar la legislación y los mecanismos de investigación a este entorno. En este sentido, los antecedentes muestran un claro reconocimiento de la importancia de contar con herramientas eficaces para combatir el cibercrimen y proteger los derechos de los ciudadanos. Los avances en materia procesal penal han llevado a la incorporación de figuras como el agente encubierto informático, cuya regulación ha planteado cuestiones controvertidas en relación con la protección de los derechos fundamentales y el control judicial de las medidas adoptadas.

Las recientes reformas en el ámbito del proceso penal han introducido dos nuevos apartados en el artículo 282 bis de la Ley de Enjuiciamiento Criminal (LECrim), estableciendo de manera novedosa la figura del agente encubierto informático. En el artículo de Alcalá, (2021), se abordarán los aspectos más polémicos que han marcado la actual regulación, en relación con la aplicación del test de legitimidad constitucional a las medidas que limitan los derechos fundamentales, así como en lo concerniente a la autorización y posterior control judicial de dichas medidas. El objetivo es arrojar luz sobre estos temas y aclarar su marco legal.

En el artículo de Cuyares, (2019), se examina la efectividad de la reciente regulación del agente encubierto informático en la aproximación de la justicia penal a la represión de este tipo de delitos. Se analizará si las disposiciones legales ofrecen un marco suficiente para combatir la delincuencia cibernética y asegurar la protección de los bienes jurídicos involucrados.

Rojas, (2023) realiza un análisis desde una perspectiva jurídica sobre el uso del agente encubierto informático como herramienta de investigación en casos de distribución de pornografía infantil en Internet. En la primera parte del texto, se lleva a cabo un estudio crítico sobre el delito de distribución de material pedófilo a través

de medios informáticos, presentando también una serie de propuestas de reforma legislativa con el objetivo de ampliar el alcance de dicho delito. En la segunda parte, se examina la figura del agente encubierto informático y se proponen modificaciones legales que permitan otorgar una mayor flexibilidad al procedimiento de autorización de este tipo de investigaciones.

En el trabajo de grado de Arévalo & Rojas, (2021) se presenta de manera clara y precisa la importancia de las herramientas de las Tecnologías de la Información y las Comunicaciones (TIC), específicamente el sistema operativo Linux en sus versiones Parrott y Kali Linux, entre otros programas. Se enfatiza en la relevancia de la seguridad informática en el avance de las investigaciones, la legislación y las tecnologías en la era digital.

El objetivo principal es mejorar los procesos investigativos mediante el uso de estas herramientas, facilitando la obtención de información e involucrando agentes informáticos para combatir los delitos cibernéticos. Además, se agradece a todas las personas que contribuyeron al avance y desarrollo de esta investigación, en particular al tutor disciplinario, el ingeniero Rolan Sosa, quien aportó sus conocimientos como policía judicial en el cuerpo técnico de investigación de la fiscalía general de la nación y brindó valiosos conocimientos sobre seguridad informática.

El agente encubierto es una institución novedosa en el Derecho Procesal Penal, que ha adquirido una importancia crucial en la legislación de varios países para combatir la delincuencia organizada. En el Ecuador, sin embargo, esta figura carece de una regulación completa, lo que ha generado preocupación debido a la posibilidad de que los agentes encubiertos cometan infracciones que vulneren derechos sin consecuencias legales, por tanto, resulta necesario establecer límites claros a esta causa de justificación.

El presente tema es de gran relevancia debido a las implicaciones actuales de las investigaciones de alto nivel llevadas a cabo por la Fiscalía General del Estado, especialmente en el contexto de la lucha contra la delincuencia organizada que se ha vuelto cada vez más difícil de combatir, especialmente cuando estas

actividades delictivas se entrelazan con esferas gubernamentales de alto nivel, lo que complica aún más la detección de infracciones.

Acosta, (2022) utiliza el método científico para proporcionar una solución viable al problema, con el objetivo de mejorar las ciencias jurídicas y proponer una reforma al inciso segundo del Art. 483 del Código Orgánico Integral Penal que delimite las circunstancias bajo las cuales los agentes encubiertos pueden ser eximidos de responsabilidad penal por las infracciones autorizadas por la ley en Ecuador. Esta propuesta ha sido sometida a la revisión y aceptación de profesionales del derecho, y se concluye que es viable y factible de implementar.

Rodríguez, (2021) analiza la aplicabilidad de los 'bots' para detectar el ciberacoso y los discursos de odio. Los 'bots' son programas informáticos diseñados para tareas específicas. Se examina su uso en conjunto con agentes encubiertos y de manera individual, considerando el marco normativo. Aunque existe escasa regulación en nuestro entorno, se pueden tomar ejemplos de derecho comparado para mejorar la legislación nacional. El ciberacoso tiene graves consecuencias, especialmente en niños y adolescentes, y es necesario abordarlo de manera efectiva.

Planteamiento del Problema

El problema se encuentra en la introducción del Agente Encubierto informático por primera vez en la legislación ecuatoriana, regulada en el Código Orgánico Integral Penal. Esta figura se incorpora a través de la "Ley orgánica reformatoria a varios cuerpos legales para el fortalecimiento de las capacidades institucionales y la seguridad integral", la cual añade la nueva figura del "agente encubierto informático" con la finalidad de investigar y esclarecer delitos. La reforma, en su artículo 77, detalla que el agente encubierto informático puede realizar tareas de gestión investigativa ocultando su verdadera identidad, patrullar el ciberespacio e infiltrarse en plataformas informáticas (Cuyares, 2019).

Sin embargo, esta implementación presenta diversas contradicciones con la normativa ecuatoriana, ya que no cumple con el principio del debido proceso. Aquí surge la duda, ¿Es viable el agente encubierto informático en el Ecuador? La falta

de una garantía que proteja el derecho al debido proceso implica una reducción de su importancia y deja a las personas en situación de indefensión en un proceso jurisdiccional, vulnerando también las obligaciones adquiridas por el Estado al ser signatario de la Convención Americana sobre Derechos Humanos.

Esta implementación no cumple con el derecho a la defensa y a la intimidad personal, lo cual plantea otro problema desde el punto de vista legal y ético. El uso de agentes encubiertos informáticos, con la capacidad de penetrar sistemas de información y acceder a datos sin autorización, pone en riesgo la privacidad de las personas y puede afectar su derecho a la defensa.

Es necesario abordar estos problemas y buscar soluciones que garanticen el respeto de los derechos fundamentales en el contexto del uso del agente encubierto informático, asegurando que se cumpla con el debido proceso, el derecho a la defensa y la protección de la intimidad personal. Esto permitirá encontrar un equilibrio entre la lucha contra el delito y el respeto a los derechos individuales en el ámbito digital (Manayalle, 2023).

La introducción del agente encubierto informático en la legislación ecuatoriana plantea diversos desafíos éticos y legales. Es fundamental abordar estos problemas de manera integral, asegurando el respeto de los derechos fundamentales, estableciendo mecanismos de control y supervisión adecuados, fomentando la transparencia y la rendición de cuentas, y garantizando la capacitación adecuada de los agentes encubiertos. De esta manera, se podrá encontrar un equilibrio entre la eficacia en la lucha contra el delito y la protección de los derechos individuales en el contexto digital (León, 2021).

Además de los problemas mencionados anteriormente, la implementación del agente encubierto informático en la legislación ecuatoriana plantea desafíos en términos de transparencia y rendición de cuentas. Dado que estas operaciones encubiertas involucran la infiltración en plataformas informáticas y la obtención de información sensible, es crucial establecer mecanismos claros de control y supervisión para prevenir abusos y garantizar la transparencia en el uso de esta herramienta.

Asimismo, es importante considerar el impacto que el uso del agente encubierto informático puede tener en la confianza de la ciudadanía en las instituciones encargadas de aplicar la justicia. Si no se establecen salvaguardias adecuadas y se cumple con los principios fundamentales del derecho penal, podría generarse una percepción de arbitrariedad y falta de imparcialidad en las investigaciones, lo que afectaría la confianza en el sistema judicial.

Adicionalmente, la implementación del agente encubierto informático plantea desafíos en cuanto a la capacitación y formación de los agentes encubiertos. Dichos deben contar con los conocimientos técnicos necesarios para operar en entornos digitales y llevar a cabo investigaciones de manera efectiva y legal. Se requiere establecer protocolos y directrices claras sobre cómo se debe realizar el uso de esta figura, a fin de evitar posibles abusos o vulneraciones de derechos.

Objetivos:

Objetivo General

- Evaluar la viabilidad de la figura del rol del agente encubierto informático en el proceso penal ecuatoriano.

Objetivos Específicos

- Analizar la legislación ecuatoriana vigente en relación al agente encubierto informático.
- Realizar un estudio comparativo con otras legislaciones con la finalidad de conocer la situación actual de la aplicación del agente encubierto.
- Elaborar propuesta de reforma legislativa con el fin de implementar la figura del agente encubierto informático.

Justificación

La implementación del Agente Encubierto Informático en la legislación ecuatoriana plantea importantes interrogantes sobre las contradicciones legales y éticas que surgen en su aplicación, así como el impacto que tiene en los derechos fundamentales de los individuos involucrados en los procesos judiciales. Este

estudio tiene como objetivo analizar a fondo estas cuestiones, identificar las contradicciones normativas y éticas, y evaluar cómo estas afectan los derechos fundamentales de las personas en el ámbito judicial.

Se examinan las disposiciones legales pertinentes, los principios éticos involucrados y se analizarán casos y precedentes para comprender las implicaciones prácticas de la implementación del Agente Encubierto informático. Al comprender y abordar estas contradicciones, se espera contribuir al debate jurídico y ético en torno al uso de esta figura en el sistema judicial ecuatoriano y proporcionar recomendaciones para salvaguardar los derechos fundamentales de los individuos involucrados en los procesos judiciales.

Si bien el uso del agente encubierto informático como técnica de investigación ha demostrado ser efectivo en varios países, también ha planteado problemas procesales debido a su carácter invasivo y a la forma en que se obtiene la información, lo cual puede resultar desproporcionado y afectar los derechos de los investigados. Por lo tanto, es necesario analizar cuidadosamente el equilibrio entre la eficacia en la lucha contra la delincuencia y el respeto de los derechos fundamentales de las personas involucradas en las investigaciones (Carrillo, 2021).

En este contexto, es importante examinar detenidamente la legislación vigente en Ecuador y realizar un estudio comparativo con las legislaciones de otros países que han regulado el rol del agente encubierto informático. Esto permitirá identificar las diferencias y similitudes en cuanto a las disposiciones legales y los mecanismos de control y supervisión existentes.

Además, se buscará elaborar una propuesta de mejora que contemple los aspectos éticos y legales involucrados en el uso del agente encubierto informático. Esta propuesta deberá abordar la necesidad de establecer límites claros para garantizar el respeto de los derechos fundamentales de los investigados, así como la implementación de mecanismos de control y supervisión adecuados para prevenir abusos y garantizar la transparencia en el uso de esta herramienta.

En la justificación de este estudio, es relevante destacar la importancia de garantizar los derechos de los ciudadanos y precautelar la seguridad en el contexto

de los procesos legales. Los principios fundamentales, como el debido proceso, la privacidad y la defensa, son pilares esenciales de cualquier sistema jurídico y su cumplimiento estricto es crucial para evitar la violación de derechos y asegurar la equidad en los procesos legales.

Si bien el agente encubierto informático ha demostrado ser una técnica efectiva en la lucha contra la delincuencia en diferentes países, su implementación plantea problemas procesales debido a su carácter invasivo y la forma en que se obtiene la información. Esto puede resultar en una falta de proporcionalidad y afectar los derechos de los investigados, lo cual es contrario a los principios del debido proceso y la protección de los derechos individuales (Hernández, 2019).

En este contexto, es necesario realizar un análisis minucioso de la legislación vigente en Ecuador en relación al agente encubierto informático, así como realizar un estudio comparativo con otras legislaciones que han regulado su uso. Esto permitirá identificar el vacío legal que existe actualmente en cuanto a las disposiciones legales y los mecanismos de control y supervisión existentes en cada jurisdicción.

Se busca elaborar una propuesta de mejora que considere tanto los aspectos éticos como legales relacionados con el uso del agente encubierto informático. Es fundamental establecer límites claros que garanticen el respeto de los derechos fundamentales de los investigados, así como implementar mecanismos de control y supervisión adecuados que prevengan abusos y aseguren la transparencia en el uso de esta herramienta.

Asimismo, es esencial considerar el impacto que puede tener el uso del agente encubierto informático en el proceso penal, tanto en términos de eficacia en la obtención de pruebas como de posibles afectaciones a los derechos procesales de los investigados. Es necesario encontrar un equilibrio que permita utilizar esta técnica de investigación de manera efectiva, sin comprometer los principios fundamentales del debido proceso y garantizando la protección de los derechos de todas las personas involucradas en los procesos legales.

CAPÍTULO I

REVISIÓN LITERATURA

1.1 El proceso penal moderno

Tras el uso de un sistema legal copiado o adaptado del acervo napoleónico milenario, Ecuador comenzó a experimentar con un sistema legal llamado abierto, que se basaba en un proceso oral. Bajo este sistema los imputados tienen derecho a conocer los cargos penales, también tienen derecho a impugnar las pruebas presentadas por la fiscalía y tienen derecho a defenderse en persona o a través de un abogado.

A lo largo de la historia ha existido un sistema llamado iniciativa. Se crearon casos individuales contra otros casos, conocidos como acusaciones, y luego se procesaron para crear un sistema que tuviera ventajas o ventajas sobre el sistema de procesamiento penal anterior (Chaúan, 2012).

Algunos perpetradores piensan que los términos acusación y lucha tienen el mismo significado, pero se debe señalar que en otras doctrinas existen diferencias históricas, legales y dogmáticas entre los dos términos, en el sentido de que no se utilizan los dos términos.

Por lo tanto, los principios del juicio oral y público pueden aplicarse en el sistema de justicia penal, ya que el juez debe evaluar injustamente la relación entre las partes en conflicto y debe estar obligado a basar su decisión en elementos fácticos.

En este sentido D´Albora (2012), describe con más detalle los elementos del sistema de pago creado en 1883. Dichos elementos se describen a continuación:

- El juicio fue realizado por los coacusados sin ninguna formación jurídica específica.
- La presencia del juez es muy importante,
- Los jueces no pueden actuar por iniciativa propia;

- La evidencia es consistente con los prejuicios y creencias de la época.

De igual forma se especifica el sistema de confidencialidad y el procedimiento escrito durante el juicio, así como las pruebas a evaluar; agregándole la figura del presidente de la Corte Suprema, siendo evidente que las facultades de defensa del imputado eran limitadas dadas por:

- Por iniciativa de los funcionarios;
- El tribunal se delega en jueces que tienen acceso a material de examen forense;
- La investigación del juez no se limita a la evidencia;
- Existe el derecho de apelación;
- La decisión se basa en pruebas legales (Agudelo Martinez, 2000).

El profesor Luigi Ferrajoli, el padre de las garantías, define un sistema de aplicación de la ley según el cual detalla cualquier sistema de procedimiento que un juez perciba como pasivo, estrictamente separado de las partes, y el procedimiento como una disputa entre partes iguales, acusación que compromete la carga de la prueba, que defiende ante sí mismo en un controvertido juicio oral y público, y que un juez pronuncia sobre su sentencia gratuita (Zavala J. , 2014).

En este sentido, los sistemas inquisitivos son mucho más que simples modelos procesales; de hecho, son expresiones de la cultura que expresan una gama de valores en la sociedad en un momento dado o en un período histórico determinado. En este contexto, los sistemas procedimentales son el resultado de la evolución de las naciones y del grado de madurez política, por lo que los cambios en estos sistemas a lo largo de la historia están vinculados a transformaciones en las instituciones. Política de Estado y justificación de las normas existentes. En cuanto al sistema acusatorio, se puede señalar que la misma lógica del Código Orgánico Integral Penal (COIP) establece que el resultado es un sistema penitenciario incoherente, impráctico y fragmentado.

El derecho penal debe garantizar la existencia de un sistema acusatorio integrado por fiscales que faciliten la comisión de los delitos conforme a los principios y motivaciones que técnicamente patrocina al acusado de un delito y las personas que, por su defensa o por su situación económica, social o cultural, no puedan utilizar los servicios de protección jurídica para defender sus derechos, así como los jueces que supervisan el proceso y garantizan los derechos de las partes interesadas (García J. , 2015).

Prieto (2017), sostiene que la contradicción como forma de juicio no tiene nada que ver con la vieja tradición causal, pero se desarrolló un enfoque radicalmente nuevo en la Inglaterra del siglo XVII.

La controversia se introdujo en los primeros conflictos laborales ingleses sobre la base de una serie de derechos procesales del acusado, como la presunción de inocencia, el derecho a guardar silencio, el derecho a escuchar testigos, etc. Profundamente inspirado por el pensamiento de la ilustración y los escritos de John Lock, los abogados de los tribunales de Inglaterra, inventaron este nuevo tipo de juicio entre 1730 y 1770 (Ruíz, 2016).

Desde este punto de vista, se podría argumentar que, según la propia Constitución, el sistema penal ecuatoriano corresponde a un sistema controvertido en el que el Estado tiene derecho a ejercer sus funciones sancionadoras y el juez Sujeto tiene una posición completamente separada de las partes. Vigilar el cumplimiento de la legislación penal y garantizar un juicio justo es la principal fuente del método de verificación de la veracidad del juicio.

Se trata, por tanto, de un juicio entre iguales iniciado por el fiscal en el que la carga de la prueba recae en el fiscal, es decir, el fiscal, estando el imputado sujeto a la presunción de inocencia, presunción intrínseca al tribunal. Por tanto, el juicio debe ser contradictorio, tanto oral como público, y el juez pondrá fin a la controversia penal según su libre condena.

1.1.1 Principios y garantías procesales:

El uso del agente encubierto informático en el proceso penal ecuatoriano debe ajustarse a los principios y garantías procesales establecidos en el sistema legal del país. Rúa, (2023) menciona algunos de los aspectos relevantes que deben ser considerados:

- **Tipicidad:** El rol del agente encubierto informático debe cumplir con el principio de tipicidad como garantía jurídica de los derechos del ciudadano, y sancionar las conductas que constituyan una infracción.
- **Proporcionalidad:** El principio de proporcionalidad implica que el uso del agente encubierto informático debe ser necesario y proporcionado en relación con la gravedad del delito investigado. Se debe evaluar si existen otras medidas menos intrusivas que puedan alcanzar el mismo objetivo investigativo antes de recurrir a esta técnica.

- **Legalidad:** La utilización del agente encubierto informático debe cumplir con los requisitos legales establecidos en la legislación penal ecuatoriana. Debe contar con una base legal clara que justifique su uso y estar sujeta a autorización judicial previa.

- **Debido proceso:** El agente encubierto informático debe ser utilizado dentro del marco del debido proceso legal. Esto implica que se deben respetar los derechos fundamentales de los involucrados, como el derecho a la defensa, el derecho a la privacidad y el derecho a un juicio justo. Se deben garantizar las garantías procesales, como la notificación, la posibilidad de impugnación y la protección de la confidencialidad de la información obtenida.

- **Protección de derechos fundamentales:** Durante la utilización del agente encubierto informático, se debe asegurar la protección de los derechos fundamentales de las personas involucradas en la investigación. Esto incluye la privacidad y la protección de datos personales, evitando cualquier uso abusivo o desproporcionado de la información obtenida.

- **Supervisión judicial:** Es necesario que la utilización del agente encubierto informático esté sujeta a una supervisión judicial efectiva. La autorización para su uso debe ser otorgada por un juez competente, quien debe evaluar y controlar la legalidad y la proporcionalidad de su utilización. Además, el juez debe recibir informes periódicos sobre el desarrollo de la operación encubierta.

- **Registro y documentación:** Todas las acciones realizadas por el agente encubierto informático deben ser registradas y documentadas de manera adecuada. Esto incluye la grabación de conversaciones, la obtención de evidencia digital y la documentación detallada de las actuaciones realizadas durante la investigación.

La utilización del agente encubierto informático en el proceso penal ecuatoriano debe cumplir con los principios y garantías procesales establecidos en la legislación del país. Es fundamental que su uso sea proporcional, legal, respete el debido proceso y proteja los derechos fundamentales de los involucrados en la investigación. La supervisión judicial y el registro adecuado de las acciones realizadas son aspectos esenciales para asegurar un uso adecuado de esta técnica investigativa.

1.1.2 El garantismo procesal

La garantía es la ideología del derecho, que es la forma de presentar, comprender, interpretar y explicar el derecho; del concepto aportado por Peredo (2007), se puede concluir que la garantía es una nueva tendencia, una nueva perspectiva teórica sobre la justicia; en este caso, la garantía corresponde al sistema implementado en la norma, que puede crear restricciones y establecer vínculos con las autoridades para proteger los derechos de los ciudadanos.

Sierra (2017), define la garantía como un método normativo de protección de los derechos subjetivos, y enfatiza que una garantía puede entenderse como una obligación correspondiente a un derecho subjetivo, lo que significa todas las expectativas legales que sean positivas o negativas.

Una de las principales propuestas del profesor italiano Luigi Ferrajoli es el desarrollo del concepto - garantía - como base de la teoría jurídica, y tiene dos significados generales: el modelo jurídico de garantía y la propuesta de una teoría jurídica general (Atienza, 2014). Como alternativa a la garantía del Estado de derecho, que limita el poder de un mismo Estado, los legisladores deben adoptar un nuevo enfoque de la teoría jurídica, ya que el Estado garante debe cambiar el paradigma clásico de los derechos por alternativas distintas a las relacionadas con el estado actual de la sociedad; y otra forma de superar una teoría positivista que debe basarse en principios filosóficos que puedan resolver problemas de legalidad, legitimidad, realidad y efectividad del derecho.

La garantía muestra la vigencia jurídica absoluta y completa de los principios que sustentan los procesos judiciales y también busca que jueces y legisladores cumplan con la Constitución y los convenios internacionales, para que las obligaciones de los jueces cumplan con el derecho procesal y de defensa; igualdad de derechos y no discriminación con el fin de preservar los derechos fundamentales efectivos.

La garantía procesal es la más importante del derecho penal, ya que esta jurisdicción brinda los aspectos más importantes de los derechos constitucionales y garantías para proteger a los ciudadanos de las imposiciones estatales (García J. , 2012). De lo anterior se puede concluir que la garantía material es consistente con el propósito del estudio de la verdad de la ley, que se basa en adaptaciones y contradicciones de los factores propuestos. En definitiva, estos principios definen un modelo de garantías o responsabilidad penal que cumple con las normas legales modernas.

Las garantías procesales no permiten que se atente o vulnere las normas básicas, otorgando los derechos de defensa adecuados, todas las partes deben respetar la paridad procesal (Intriago, 2014). De lo dicho se puede concluir que, en un estado constitucional de derecho, la garantía es el sistema más adecuado para suspender o limitar las sanciones impuestas por el estado a través de las instituciones, para que las normas cumplan con el marco mínimo para el derecho penal.

1.2 Delitos cibernéticos

El Convenio sobre la Ciberdelincuencia, también conocido como Convenio de Budapest, ha sido aprobado por el Consejo de Europa y cuenta con la ratificación de más de 56 países, incluyendo no europeos. Este convenio tiene como objetivo promover la cooperación internacional en la lucha contra los delitos informáticos que se cometen en el ciberespacio. El Convenio de Budapest aborda la armonización del derecho penal sustantivo en materia de delitos cibernéticos, establece parámetros procesales mínimos para la investigación y sanción de estas conductas, y crea mecanismos de cooperación a nivel europeo (Montalbano, 2019).

Aunque Ecuador no es parte de este convenio, el país ha dado importancia creciente a la atención del cibercrimen. En octubre de 2008, se llevó a cabo un evento titulado "Cibercriminalidad en Ecuador", que tuvo como objetivo analizar los delitos informáticos más frecuentes en América Latina, como violaciones a la propiedad intelectual, delitos en el comercio electrónico y pornografía infantil (Guix, 2022).

El Código Orgánico Integral Penal (COIP) no regula de manera específica la ciberdelincuencia, pero identifica ciertas conductas que podrían cometerse utilizando medios informáticos. Sin embargo, la doctrina consultada señala que la protección de la integridad, disponibilidad y accesibilidad de los sistemas informáticos y los datos alojados en ellos solo ha sido abordada de manera excepcional en el COIP.

En la lucha contra los ciberdelincuentes, INTERPOL proporciona apoyo operativo, investigativo, inteligencia cibernética, análisis forense digital, innovación e investigación. Ecuador, como miembro activo de INTERPOL, puede aprovechar las oportunidades tecnológicas que ofrece esta organización internacional para enfrentar las ciber amenazas, especialmente aquellas que afectan a niños, niñas y adolescentes.

EUROPOL y su Centro Europeo de Ciberdelincuencia (EC3) también se han aliado con INTERPOL para abordar los desafíos de perseguir actividades ilegales en línea. El Informe de la IOCTA 2017 destaca algunos éxitos operativos en la lucha

contra el ciberdelito, como la eliminación de los principales mercados de la Darknet y el desmantelamiento de la red Avalancha. Sin embargo, se enfatiza la necesidad de una legislación específica que permita la acción de la ley en el entorno en línea (C. Hernández, 2021).

La preocupación por la ciberdelincuencia y los delitos sexuales contra niños, niñas y adolescentes en el ciberespacio ha llevado a discusiones sobre la necesidad de contar con legislación adaptada y de mejorar la cooperación internacional. La jurisdicción y la competencia son temas complejos debido a la naturaleza transnacional de estos delitos, lo que requiere una interacción entre los operadores de justicia de diferentes países.

Dada la creciente ciberdelincuencia y la evidencia electrónica relacionada, es necesario abordar la jurisdicción y la competencia en este ámbito y promover la cooperación internacional. En el ciberespacio, donde la delincuencia opera a nivel global, es fundamental ampliar la concepción y el alcance del agente encubierto para recabar información y combatir estos delitos de manera efectiva (Fuentes, 2022).

1.3 Técnicas Especiales de Investigación

Se encuentran reguladas en la sección tercera del libro segundo del Código Orgánico Integral Penal (COIP) de Ecuador, que está en vigencia desde el 10 de agosto de 2014. En esta sección se establecen disposiciones relacionadas con la interceptación de comunicaciones o datos informáticos (artículos 476 y siguientes) y las operaciones investigativas con agentes encubiertos e informantes (artículos 483 y siguientes). Aunque el COIP no proporciona una definición específica de las Técnicas Especiales de Investigación, la formulación utilizada en la norma se asemeja a la contenida en la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (Jácome, 2019).

Las Técnicas de Investigación Especiales son denominadas así porque su utilización puede implicar la lesión o vulneración de derechos fundamentales de los ciudadanos. Por esta razón, su empleo debe ser considerado de manera "especial"

o, según lo establecido en la norma penal, "excepcional", y sólo puede ser autorizado cuando exista una amplia justificación para ello.

Dentro del catálogo de Técnicas de Investigación Especiales, los agentes encubiertos ocupan un lugar destacado en términos de estudio, ya que la cantidad de derechos que se ven afectados en estas operaciones solo puede ser justificada por la necesidad de detectar presuntos delitos y aprehender a los delincuentes involucrados (León, 2021).

1.4 El agente encubierto informático

En Ecuador, el agente encubierto es un servidor policial o fiscal cuyo historial personal y profesional es conocido. Según la definición de Molina Pérez, el agente infiltrado es un funcionario de la policía que actúa de manera encubierta en un ambiente criminal específico para reprimir y prevenir delitos, así como descubrir a los miembros de la organización criminal, llevando a cabo tareas y funciones atribuidas por la ley. El agente encubierto se involucra directamente con la organización delictiva con el objetivo de obtener la mayor cantidad posible de información sobre las personas involucradas y las posibles infracciones cometidas o por cometer (Manayalle, 2023).

Por otro lado, el informante es cualquier persona que proporciona información a la fiscalía o al personal del Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses sobre la preparación o comisión de un delito, así como sobre las personas que han participado en él. Tanto en el caso del agente encubierto como en el del informante, la identidad de estas personas está protegida y revelarla constituye un delito tipificado y sancionado en el COIP (artículo 273) (Asamblea Nacional del Ecuador, 2008).

En la doctrina extranjera se hace referencia al confidente, que se entiende como una persona que proporciona información a quienes están a cargo de una investigación penal y obtiene ciertas ventajas a cambio. Puede estar dentro o fuera de una organización, pero su objetivo no es provocar delitos ni infiltrarse para investigar, como lo haría un agente encubierto según la definición de Molina Pérez.

La actividad de los agentes encubiertos, tal como se establece en la legislación ecuatoriana, se centra principalmente en la recopilación de información y elementos de prueba utilizando una identidad ficticia. No se plantea que el agente pueda provocar situaciones delictivas, aunque la doctrina consultada señala que se podría instigar, convirtiéndose así en un agente provocador.

El agente encubierto informático es una figura utilizada en el ámbito de la investigación penal para combatir delitos informáticos y obtener pruebas de relevancia en el proceso penal. Se trata de un individuo o equipo especializado que, de manera encubierta, se infiltra en redes o plataformas digitales con el fin de recopilar información, identificar a los responsables de los delitos y obtener pruebas válidas para su presentación ante los tribunales (Bravo, 2021).

Este agente encubierto informático puede adoptar diversas identidades y perfiles falsos en línea para interactuar con los sospechosos y obtener información clave sobre actividades delictivas. Puede llevar a cabo actividades como el monitoreo de comunicaciones, el acceso a sistemas protegidos, el seguimiento de transacciones y la recopilación de evidencia digital.

La utilización del agente encubierto informático es particularmente relevante en delitos informáticos como el fraude en línea, la pornografía infantil, el cibercrimen, el robo de información confidencial y otros delitos cometidos a través de medios digitales. Su principal objetivo es recopilar pruebas que permitan la persecución y sanción de los responsables, contribuyendo así a la prevención y represión de estos delitos.

Es importante destacar que el agente encubierto informático debe operar dentro del marco legal establecido, respetando los derechos fundamentales de los involucrados y cumpliendo con los procedimientos y garantías procesales correspondientes. Su utilización está sujeta a regulaciones específicas en cada país, las cuales establecen los límites y requisitos para su empleo, garantizando la proporcionalidad y la legalidad en su accionar (Segovia, 2022).

La intervención del agente encubierto ha evolucionado para adaptarse al entorno cibernético, donde ya no se limita a una circunscripción territorial, sino que

se convierte en un agente encubierto cibernético, digital, online o informático. En este nuevo entorno, el agente lleva a cabo operaciones encubiertas en el espacio virtual, aprovechando el anonimato y la identidad virtual que proporciona Internet.

El agente encubierto en Internet utiliza perfiles falsos para ocultar su verdadera identidad policial y establecer relaciones de confianza con los ciberdelincuentes, con el objetivo de obtener información para desenmascarar a los criminales. Esta figura se vuelve especialmente relevante en la persecución de delitos cibernéticos como el grooming, el ciberacoso y el morphing.

La actuación del agente encubierto cibernético presenta desafíos únicos, ya que los delincuentes cibernéticos operan en un entorno virtual que es ilimitado, exuberante y descentralizado. Es crucial que el agente encubierto en este entorno sea invisible y universal para prevenir y combatir el crimen en línea. Sin embargo, su actuación debe respetar los principios y límites legales establecidos.

En la lucha contra la ciberdelincuencia, se utilizan herramientas técnicas y tecnológicas para identificar y rastrear a los delincuentes. Se realiza un monitoreo constante de los sitios web y se utilizan software y programas especializados para la geolocalización de las direcciones IP y la identificación de redes de intercambio de archivos ilegales. Aunque el intercambio de material pornográfico infantil aún ocurre en redes peer-to-peer y en la Deep Web, se están realizando esfuerzos para combatir estas actividades delictivas (García, 2021).

La actuación del agente encubierto cibernético requiere el uso de anzuelos y trampas para atraer a los delincuentes en línea. En el caso específico de la pornografía infantil, por ejemplo, el agente puede aparentar ser un usuario que posee contenido ilegal para ganarse la confianza de los delincuentes. Sin embargo, estas actuaciones deben estar respaldadas por autorización judicial, ya que implican la vulneración de derechos fundamentales como el secreto de las comunicaciones. Su labor en el espacio virtual requiere adaptarse a las particularidades de este entorno, utilizando técnicas de investigación específicas para desmantelar redes delictivas y proteger a los ciudadanos en línea. Sin embargo, es importante garantizar que su actuación esté regulada por la ley y respete los derechos fundamentales.

1.4.1 Finalidad y justificación del agente encubierto informático:

La finalidad del agente encubierto informático en el proceso penal es la obtención de pruebas relevantes para esclarecer delitos y perseguir la comisión de actividades delictivas en el ámbito digital. Esta herramienta investigativa se utiliza para infiltrarse en redes delictivas y obtener información que permita identificar a los responsables, recopilar pruebas y desmantelar organizaciones criminales.

La justificación del agente encubierto informático radica en la necesidad de adaptar las técnicas de investigación a los avances tecnológicos y al creciente uso de las comunicaciones electrónicas en la comisión de delitos. El agente encubierto informático permite investigar delitos informáticos, ciberdelitos, fraudes electrónicos, delitos contra la propiedad intelectual, entre otros, que se perpetran a través de medios electrónicos o en el entorno digital. (López, 2023).

Además, el agente encubierto informático puede contribuir a prevenir delitos al anticiparse a las acciones delictivas y detectar planes criminales en etapas tempranas. Esta herramienta puede resultar especialmente efectiva en casos donde las pruebas son difíciles de obtener de manera convencional debido a la naturaleza encubierta de las actividades delictivas en línea.

Es importante destacar que el uso del agente encubierto informático debe estar sujeto a estrictos controles legales y garantías procesales para salvaguardar los derechos fundamentales de las personas, como el derecho a la privacidad y el debido proceso. La proporcionalidad y la necesidad de utilizar esta técnica deben ser evaluadas caso por caso, considerando los principios de legalidad, proporcionalidad y respeto a los derechos humanos (Carrillo, 2021).

1.4.2 Validación científica y técnica del agente encubierto informático:

La validación científica y técnica del agente encubierto informático es fundamental para asegurar su eficacia y confiabilidad en el proceso penal ecuatoriano. Cutire, (2023) señala que esta validación implica dos aspectos principales:

- **Validación científica:** Se refiere a la verificación de la fundamentación científica y teórica del agente encubierto informático. Esto implica evaluar si los principios y métodos utilizados en su desarrollo están respaldados por investigaciones científicas, estudios empíricos y conocimientos técnicos especializados. Se deben considerar aspectos como la confiabilidad de los sistemas utilizados, la precisión de los algoritmos y las técnicas de recolección y análisis de datos.

- **Validación técnica:** Se refiere a la comprobación de la operatividad y eficiencia del agente encubierto informático en la práctica. Esto implica evaluar su capacidad para obtener información relevante y fiable, su capacidad para adaptarse a diferentes contextos y situaciones, así como su interoperabilidad con otros sistemas y tecnologías utilizadas en el proceso penal. También se deben considerar aspectos de seguridad informática, como la protección de datos y la prevención de vulnerabilidades.

La validación científica y técnica del agente encubierto informático debe realizarse a través de estudios y pruebas rigurosas, preferiblemente llevadas a cabo por expertos en el campo de la informática forense y la investigación criminal. Estas pruebas deben seguir estándares y protocolos reconocidos internacionalmente para garantizar la calidad y confiabilidad de los resultados.

Además, es importante que exista transparencia en la validación del agente encubierto informático, de modo que los resultados y las limitaciones del sistema sean comunicados de manera clara y comprensible a los actores del sistema de justicia penal, incluyendo a los jueces, fiscales y defensores.

En resumen, la validación científica y técnica del agente encubierto informático es esencial para garantizar su eficacia y confiabilidad en el proceso penal ecuatoriano. Esto implica evaluar su fundamentación científica, su operatividad y su capacidad de adaptación a diferentes contextos. La realización de pruebas y estudios rigurosos, siguiendo estándares reconocidos, es clave para asegurar su validez en el ámbito jurídico y su aceptación por parte de los operadores de justicia.

1.4.3 Consideraciones éticas y legales del uso del agente encubierto informático

En el ámbito del empleo del agente encubierto informático, emergen cuestiones éticas y legales de suma relevancia que requieren ser consideradas detenidamente. Uno de los aspectos primordiales se relaciona con la salvaguardia de la privacidad y los derechos fundamentales de las personas implicadas en las investigaciones. Aunque el agente encubierto puede constituir una herramienta eficaz en la lucha contra el delito, resulta imperativo asegurar que su utilización no menoscabe los derechos individuales y se adhiera al principio de proporcionalidad.

Asimismo, es necesario establecer mecanismos adecuados de control y supervisión que garanticen que el agente encubierto opere dentro de los límites legales y éticos establecidos. Esto implica la definición de procedimientos claros para la autorización y supervisión de las operaciones encubiertas, así como la asignación de responsabilidades tanto para los agentes encubiertos como para las autoridades pertinentes (Asencio, 2022).

Resulta esencial establecer límites y restricciones para asegurar un uso apropiado y proporcionado del agente encubierto informático. Este aspecto conlleva la precisa delimitación de los delitos susceptibles de ser investigados mediante esta herramienta, así como la definición de criterios para determinar la necesidad y justificación de su empleo en cada caso.

El conflicto surge al momento de que el estado implementa esta figura con el fin de combatir el cibercrimen fortaleciendo el estado de defensa y contribuir al fortalecimiento de las capacidades institucionales en la búsqueda de la seguridad integral, puesto que, la duda de la vulneración de los derechos y principios nace con respecto a los límites del agente encubierto informático con la privacidad de los ciudadanos.

La ponderación de derechos entra cuando se presenta un conflicto entre principios, puesto que, debe haber un balance con el fin de confrontar y resolver los conflictos que contraiga el rol del agente encubierto informático, pues se buscará dar una tutela real y efectiva a fin de determinar cuál deberá prevalecer sobre el otro

y verificar cuál de ellas permite una mejor efectividad. La ponderación es una herramienta vital si se pretende que la Constitución, garantías y derechos fundamentales se cumplan a cabalidad.

El uso del agente encubierto informático plantea desafíos éticos y legales que demandan una aproximación cautelosa y rigurosa. Es imprescindible encontrar un equilibrio entre la eficacia en la lucha contra el delito y la protección de los derechos individuales, garantizando que su utilización se enmarque dentro de los límites establecidos por la legislación y los principios éticos (Cutrona, 2023).

1.4.4 El agente encubierto informático en el contexto de la era digital

En la era digital en la que se vive, donde el ciberespacio se ha convertido en un territorio repleto de amenazas y ataques constantes, la necesidad de proteger nuestra información y salvaguardar la seguridad de nuestros sistemas informáticos es más apremiante que nunca. La creciente dependencia de la tecnología y la interconexión global han dado lugar a un aumento significativo de delitos cibernéticos, como el robo de datos, el fraude en línea y el acceso no autorizado a sistemas informáticos (Ramos, 2021).

En la era digital, la protección de la información y la seguridad de los sistemas informáticos son temas de gran importancia debido a la creciente amenaza de los delitos cibernéticos, el avance de la tecnología ha facilitado la conectividad global, pero también ha dado lugar a nuevas oportunidades para los delincuentes en línea.

El robo de datos, el fraude en línea y el acceso no autorizado a sistemas informáticos son solo algunas de las muchas formas en que los delincuentes cibernéticos pueden causar daño. Dichos ataques pueden tener consecuencias graves, tanto para los individuos como para las organizaciones, ya que pueden resultar en la pérdida de información confidencial, la interrupción de servicios, el daño a la reputación y pérdidas financieras significativas.

La protección contra los delitos cibernéticos implica la implementación de medidas de seguridad sólidas en diferentes niveles. Esto incluye el uso de software

de seguridad actualizado, el cifrado de datos, la autenticación de dos factores, la educación y concienciación sobre las mejores prácticas de seguridad, y la colaboración entre los sectores público y privado para compartir información y desarrollar estrategias de defensa.

En este contexto, la figura del agente encubierto informático se ha vuelto fundamental en la lucha contra la delincuencia digital. Su labor consiste en infiltrarse en grupos delictivos en el ámbito digital, recopilar información, desmantelar operaciones ilegales y prevenir futuros ataques delictivos. Al trabajar en el ciberespacio, donde las amenazas pueden ser difíciles de detectar y combatir, el agente encubierto informático desempeña un papel crucial en la identificación y persecución de los delincuentes en el mundo virtual (Morinelly, 2021).

Además, es esencial que las leyes y regulaciones se adapten al entorno digital para poder perseguir y sancionar de manera efectiva a los delincuentes cibernéticos. Esto implica una cooperación internacional en la lucha contra el cibercrimen, ya que los ataques pueden originarse en diferentes partes del mundo.

1.4.5 El papel del agente encubierto informático en la protección y persecución de delitos cibernéticos

Ante la creciente amenaza de los delitos cibernéticos, el agente encubierto informático se ha convertido en una herramienta vital en la lucha contra la delincuencia digital. Dichos agentes son expertos en el manejo de la tecnología y en las artes del disfraz digital, lo que les permite infiltrarse en redes criminales y descubrir sus operaciones ilegales.

El agente encubierto informático opera bajo una identidad falsa en canales de comunicación cerrados, donde se llevan a cabo actividades delictivas. Su objetivo principal es recopilar información, obtener pruebas de los delitos cometidos y facilitar el desmantelamiento de las operaciones criminales. Para lograr esto, el agente encubierto informático puede comunicarse, intercambiar archivos e incluso enviar archivos ilícitos, siempre que cuente con la debida autorización judicial (S. Hernández, 2019).

Los agentes encubiertos informáticos se han vuelto una herramienta crucial en la lucha contra los delitos cibernéticos. Dichos agentes especializados poseen conocimientos avanzados en tecnología y técnicas de infiltración en línea, lo que les permite adentrarse en redes criminales y recopilar información sobre actividades ilegales.

La identidad falsa utilizada por los agentes encubiertos informáticos les proporciona una capa de protección al interactuar en canales de comunicación cerrados donde se llevan a cabo actividades delictivas. Esta identidad falsa les permite ganarse la confianza de los delincuentes y obtener acceso a información crucial para investigaciones posteriores (Fuentes, 2022). El objetivo principal de un agente encubierto informático es recopilar pruebas y evidencias de los delitos cibernéticos cometidos por las organizaciones criminales. Estas pruebas son fundamentales para llevar a cabo acciones legales y desmantelar las operaciones criminales.

Es importante destacar que los agentes encubiertos informáticos deben actuar dentro de los límites legales y contar con la debida autorización judicial. Aunque puedan comunicarse, intercambiar archivos e incluso enviar archivos ilícitos como parte de su labor encubierta, siempre deben seguir los procedimientos legales y respetar los derechos de las personas involucradas.

En resumen, los agentes encubiertos informáticos desempeñan un papel crucial en la lucha contra los delitos cibernéticos al infiltrarse en redes criminales, recopilar pruebas y facilitar el desmantelamiento de las operaciones ilegales. Su labor requiere conocimientos técnicos avanzados y el cumplimiento estricto de las leyes y regulaciones aplicables.

1.4.6 Regulación y supervisión del uso del agente encubierto informático

Con el objetivo de garantizar la efectiva incorporación del agente encubierto cibernético en el marco legal, se proponen dos elementos clave para la posible reforma legislativa. Es necesario que la legislación defina de manera precisa qué se entiende por agente encubierto cibernético, sus funciones, límites y

responsabilidades, lo cual permitirá evitar ambigüedades y asegurar que el uso de estos agentes se realice dentro de los límites legales establecidos.

En primer lugar, es necesario considerar el ámbito espacial en el que pueden llevarse a cabo estas operaciones encubiertas. Dado que los delitos cibernéticos trascienden las fronteras y tienen lugar en la profundidad de la Web, que abarca múltiples países, resulta fundamental que Ecuador se adhiera al Convenio de Budapest u otros tratados internacionales que promueven la cooperación y colaboración entre cuerpos de seguridad de distintas naciones en la lucha contra los delitos cibernéticos. Esto permitiría una persecución internacional de estos delitos y una mayor efectividad en las operaciones encubiertas en Internet (Moyano, 2021).

En segundo lugar, es necesario otorgar facultades amplias al agente encubierto cibernético. Estas facultades requerirán una ampliación de las formas tradicionales establecidas en la legislación. Será necesario modificar el contenido de los artículos 480 y 482, así como el numeral 3 del artículo 484 del COIP, que se refieren al allanamiento, su procedimiento y las reglas de las operaciones encubiertas. En particular, se deberá establecer que el agente encubierto cibernético puede intercambiar información y ganarse la confianza de los delincuentes en redes delictivas virtuales, siempre y cuando no impulse delitos que no sean de iniciativa previa de los investigados.

Estas reformas son fundamentales para combatir la diversidad de delitos cibernéticos, que trascienden el ámbito territorial de Ecuador y requieren de una acción coordinada a nivel internacional. A pesar de la importancia del agente encubierto informático en la lucha contra los delitos cibernéticos, su uso plantea desafíos éticos y legales. Es fundamental establecer límites claros y garantizar que su actuación se realice dentro del marco legal, respetando los derechos y libertades individuales.

En Ecuador, la figura del agente encubierto informático está regulada por el Código Orgánico Integral Penal (COIP) y requiere de autorización judicial para su empleo. La identidad supuesta del agente y su participación en canales cerrados de comunicación deben ser debidamente controlados y supervisados. Además, se establecen límites en cuanto a la duración de la medida y la exención de

responsabilidad penal del agente encubierto informático, que solo se aplica a aquellos actos indispensables para el progreso y resultado de la investigación (Pino, 2019).

1.5 Legislación Comparada

1.5.1 Agente Encubierto Informático: Ecuador Vs. España

En la legislación de España presenta una normativa más desarrollada en cuando a las funciones del agente encubierto informático, el cual procede en los siguientes tipos delictuales:

- Cuando se trate de investigaciones de actividades de la delincuencia organizada.
- Delitos de obtención, tráfico de órganos humanos, secuestro de personas y trata de seres humanos.
- Delitos relativos a la prostitución.
- Delitos contra el patrimonio.
- Delitos relativos a la propiedad intelectual e industrial.
- Delitos contra los derechos de los trabajadores.
- Delitos contra los derechos de los ciudadanos extranjeros.
- Delitos de tráfico nuclear, radiactivo, depósito de armas, municiones o explosivos.
- Delitos contra la salud pública.
- Delitos de falsificación de moneda, tarjetas de crédito o cheques de viaje.
- Delitos de terrorismo.
- Delitos contra el patrimonio histórico.

Se puede observar que el agente encubierto informático posee una amplia expansión de delitos en cuanto a su competencia. Por otro lado, en la normativa española existen restricciones para establecer un mejor control en cuanto a esta figura, se establece que el juez es el único que puede autorizar a los Policías Judiciales para que puedan desempeñar como agente encubierto informático, el cual deberá incluir el nombre real del funcionario y su nombre de identidad falsa y

datos personales básicos, la autorización tendrá un plazo de 6 meses, con opción de prórroga por el mismo período. Dentro de sus facultades otorgadas podrá:

- Grabar de manera íntegra las conversaciones como soporte, el cual deberá ser remitido al juzgado donde reposarán las grabaciones.
- Deberán adoptarse las debidas medidas de control con el fin de asegurarse que no se producirá ningún comportamiento que pueda ser un delito por parte del agente encubierto.
- Toda información que recopile el agente encubierto informático deberá ser de carácter reservado y expuesto en conocimiento ante el juzgado a la mayor brevedad para valorar su conformidad.

Sin embargo, en el Ecuador por ser una nueva figura en la normativa existen muchos vacíos legales, en el artículo 77 de la Ley Orgánica Reformatoria a varios cuerpos legales para el fortalecimiento de las capacidades institucionales y la seguridad integral, que modifica el artículo 483 del Código Orgánico Integral Penal (COIP) establece que este nuevo rol podrá realizar patrullajes o acciones digitales en el ciberespacio, el cual dentro de sus facultades podrá:

- Infiltrarse en plataformas digitales como foros, grupos de comunicación, fuentes cerradas de comunicación.
- Acceder a la información sin la autorización de los dueños de los datos.
- Intercambiar y enviar información de contenido ilícito con el fin de recolectar información útil para la investigación.
- Infectar con Malware espía.
- Realizar compras controladas con el objetivo de descubrir algún hecho delictivo cometido en alguna plataforma digital.

La reforma ecuatoriana es mucho más amplia que la normativa española, ya que el agente encubierto informático puede proceder sólo con la autorización del fiscal, por otro lado, solo se establecieron dos límites a los agentes encubiertos informáticos, el cual no podrán impulsar delitos que no sean de iniciativa de las personas investigadas salvo en caso de compras controladas y sólo podrá utilizar su identidad encubierta por un periodo de dos años y hasta después de la audiencia de juicio.

1.6 Marco legal y normativo en Ecuador:

En Ecuador, la utilización del agente encubierto informático en el proceso penal está regulada por diversas leyes y normativas que establecen los procedimientos, requisitos y límites para su viabilidad. Algunas de las leyes y normativas relevantes en este contexto son las siguientes:

El Código Orgánico Integral Penal (COIP) establece los principios generales y las normas aplicables al proceso penal en Ecuador. En su Título III, Capítulo 3, se abordan las disposiciones relativas a la investigación y los medios de prueba. En este marco, se establecen los principios de legalidad, proporcionalidad y garantía de derechos fundamentales que deben ser respetados en la utilización del agente encubierto informático. El Código Orgánico Integral Penal (COIP) en Ecuador es la normativa legal que establece los principios generales y las normas aplicables al proceso penal en el país. En su Título III, Capítulo 3, se abordan las disposiciones relativas a la investigación y los medios de prueba, incluyendo las regulaciones específicas para el uso del agente encubierto informático.

Dentro de este marco normativo, se establecen principios fundamentales que deben ser respetados en la utilización del agente encubierto informático. Uno de ellos es el principio de legalidad, que implica que el uso de esta técnica especial de investigación tecnológica debe estar respaldado por una autorización judicial expresa y específica. Esto garantiza que la actuación encubierta esté dentro de los límites establecidos por la ley y que se respeten los derechos y garantías de las personas involucradas.

Además, se establece el principio de proporcionalidad, el cual implica que las acciones del agente encubierto informático deben ser adecuadas y necesarias para lograr los fines de la investigación. Esto significa que la infiltración en grupos delictivos y la recopilación de información deben ser proporcionales a la gravedad y naturaleza de los delitos investigados. La proporcionalidad busca evitar cualquier exceso o abuso en el ejercicio de las facultades del agente encubierto informático.

Asimismo, se garantiza el respeto de los derechos fundamentales de las personas involucradas en la investigación. Esto implica que, a pesar de la actuación

encubierta, se deben salvaguardar los derechos a la intimidad, al secreto de las comunicaciones y a la presunción de inocencia. El agente encubierto informático debe actuar dentro de los límites legales establecidos, evitando cualquier vulneración injustificada de los derechos de los usuarios involucrados en los canales de comunicación cerrados.

En el marco legal del COIP, se establece la necesidad de controlar y supervisar adecuadamente la actuación del agente encubierto informático. Esto implica que la autorización judicial debe contemplar los límites y alcances de la infiltración, así como la duración de la medida. Además, se deben establecer mecanismos de control y supervisión para evitar abusos y garantizar que la actuación del agente encubierto informático se ajuste a los principios de legalidad, proporcionalidad y respeto a los derechos fundamentales (Aveiga et al., 2021).

La ley Orgánica de Telecomunicaciones regula el uso de las telecomunicaciones en Ecuador y establece los mecanismos para la cooperación entre proveedores de servicios de telecomunicaciones y las autoridades competentes en materia de investigación penal. En el contexto del agente encubierto informático, esta ley puede ser relevante para obtener la colaboración de los proveedores de servicios en la obtención de información necesaria para la investigación.

En el contexto del agente encubierto informático, la Ley Orgánica de Telecomunicaciones puede ser relevante en cuanto a la cooperación entre los proveedores de servicios de telecomunicaciones y las autoridades competentes en materia de investigación penal. La ley establece la obligación de los proveedores de servicios de telecomunicaciones de colaborar con las autoridades en la investigación de delitos y facilitar el acceso a la información necesaria para dichas investigaciones.

En este sentido, los proveedores de servicios de telecomunicaciones pueden ser requeridos para brindar información sobre las comunicaciones realizadas a través de sus redes, como registros de llamadas, registros de mensajes de texto, datos de conexión a internet, entre otros. Esta colaboración es fundamental para

que las autoridades puedan recabar las pruebas necesarias en el marco de la investigación penal y el uso del agente encubierto informático.

Es importante destacar que la cooperación entre los proveedores de servicios de telecomunicaciones y las autoridades debe realizarse dentro de los límites establecidos por la ley y respetando los derechos de privacidad de los usuarios. La Ley Orgánica de Telecomunicaciones establece salvaguardias para proteger la confidencialidad de la información de los usuarios y garantizar que su acceso y uso esté sujeto a un control judicial adecuado (Guamán, 2023).

La Ley de Protección de Datos Personales establece las disposiciones para la protección de la privacidad y los datos personales de los individuos. En el contexto del agente encubierto informático, es importante garantizar que la recopilación y el uso de datos se realicen de acuerdo con las disposiciones legales establecidas y que se respeten los derechos de privacidad de las personas involucradas.

En el contexto del agente encubierto informático, es esencial garantizar que cualquier recopilación y uso de datos personales se realice de acuerdo con las disposiciones legales establecidas en la Ley de Protección de Datos Personales. Esto implica que las autoridades competentes deben cumplir con los principios de legalidad, consentimiento, finalidad, proporcionalidad y seguridad al utilizar los datos obtenidos a través de la actuación del agente encubierto informático.

La ley establece que la recopilación y tratamiento de datos personales sólo pueden llevarse a cabo con el consentimiento del titular de los datos, a menos que exista una base legal para su procesamiento. En el caso del agente encubierto informático, se debe asegurar que cualquier recolección de datos se realice dentro del marco legal establecido y con el consentimiento adecuado cuando sea requerido.

Además, la Ley de Protección de Datos Personales establece los derechos de los titulares de datos, como el derecho de acceso, rectificación, cancelación y oposición al tratamiento de sus datos personales. Dichos derechos deben ser respetados incluso en el contexto de la investigación penal y el uso del agente

encubierto informático. Se deben establecer mecanismos para que los individuos puedan ejercer sus derechos en relación con los datos recopilados durante la investigación.

Es importante destacar que el uso del agente encubierto informático no puede ser una excusa para el incumplimiento de la Ley de Protección de Datos Personales. Las autoridades competentes deben asegurarse de que cualquier actividad realizada por el agente encubierto esté sujeta a los principios y disposiciones legales establecidas en esta ley, y que se implementen las medidas de seguridad necesarias para proteger los datos personales recopilados (Caycho & Saguma, 2021).

El Reglamento General de la Ley de Telecomunicaciones complementa la Ley Orgánica de Telecomunicaciones y establece las obligaciones específicas de los proveedores de servicios de telecomunicaciones en relación con la colaboración con las autoridades competentes en la investigación penal.

En el contexto del agente encubierto informático, el Reglamento General de la Ley de Telecomunicaciones es relevante para regular la cooperación entre los proveedores de servicios de telecomunicaciones y las autoridades competentes en la obtención de información necesaria para la investigación penal. Estas disposiciones buscan garantizar que los proveedores de servicios de telecomunicaciones brinden la colaboración requerida y faciliten el acceso a la información relevante.

La ley establece que los proveedores de servicios de telecomunicaciones deben colaborar con las autoridades competentes en la investigación penal, proporcionando la información necesaria dentro de los plazos establecidos. Esto incluye la entrega de registros de comunicaciones, datos de tráfico y cualquier otra información relevante que pueda contribuir a la investigación.

Sin embargo, es importante señalar que la obtención y uso de esta información debe realizarse de acuerdo con los principios del debido proceso y respetando los derechos fundamentales consagrados en la Constitución ecuatoriana, como el derecho a la privacidad. En este sentido, el papel del agente

encubierto informático es crucial, ya que permite a las autoridades recoger evidencia de manera eficaz y eficiente, sin violar los derechos de los individuos.

Además, se establecen regulaciones para garantizar la seguridad e integridad de la información obtenida. Los proveedores de servicios de telecomunicaciones deben garantizar que los datos recopilados se mantengan seguros y solo sean accesibles para las autoridades competentes. De igual forma, los agentes encubiertos informáticos están obligados a manejar y utilizar la información recogida de manera responsable y solo para los fines de la investigación.

El Reglamento General de la Ley de Telecomunicaciones provee un marco normativo importante para el funcionamiento del agente encubierto informático en Ecuador, estableciendo obligaciones claras para los proveedores de servicios de telecomunicaciones y garantizando que se respeten los derechos de los ciudadanos en el proceso de investigación penal.

Además, la ley establece los procedimientos y requisitos que deben seguir las autoridades competentes al solicitar información a los proveedores de servicios de telecomunicaciones. Estas solicitudes deben estar debidamente fundamentadas y deben cumplir con los requisitos legales establecidos para garantizar la protección de los derechos de las personas involucradas.

Es importante destacar que la Ley de Telecomunicaciones también aborda la confidencialidad de la información proporcionada por los proveedores de servicios de telecomunicaciones. Establece que la información entregada en el contexto de una investigación penal debe ser tratada de manera confidencial y utilizada únicamente para los fines establecidos en la solicitud (Vinueza, 2021).

Es fundamental que el uso del agente encubierto informático en el proceso penal se realice de acuerdo con estas leyes y normativas, respetando los derechos fundamentales de los individuos, la proporcionalidad en la obtención de pruebas y cumpliendo con los procedimientos establecidos. Asimismo, es importante que existan salvaguardias y controles adecuados para evitar abusos y garantizar la transparencia y la legalidad en su utilización.

CAPÍTULO II

METODOLOGÍA DE LA INVESTIGACIÓN

1.1 Diseño de la investigación

En el caso del estudio de la viabilidad del uso de un Agente Encubierto Informático en el proceso penal ecuatoriano, será enfocada en una investigación cualitativa para obtener una comprensión completa del tema.

En este enfoque, se pueden utilizar métodos cualitativos, como entrevistas a expertos en derecho penal, tecnología y agencias de aplicación de la ley, para obtener perspectivas y opiniones sobre la viabilidad del uso de un Agente Encubierto Informático. Estas entrevistas exploran las experiencias, conocimientos y puntos de vista de los profesionales involucrados en el proceso penal y proporcionar información detallada y contextualizada sobre los desafíos y consideraciones éticas relacionadas con este tipo de investigación. Esto permitirá identificar patrones, tendencias y desafíos comunes, así como comprender las perspectivas y experiencias de los actores involucrados en el sistema legal y de justicia.

Es importante tener en cuenta que la investigación cualitativa requiere una cuidadosa planificación y ejecución, así como la selección apropiada de métodos cualitativos en función de los objetivos de investigación. Además, es esencial considerar las limitaciones y sesgos potenciales del método cualitativa y realizar un análisis riguroso de los datos recopilados para obtener conclusiones válidas y confiables.

1.2 Tipo de investigación

La presente investigación tiene como objetivo analizar la viabilidad del uso del agente encubierto informático en el proceso penal ecuatoriano. Se trata de un estudio descriptivo que busca explorar las implicaciones y beneficios de esta técnica investigativa en la lucha contra los delitos informáticos y su aplicación dentro del marco legal ecuatoriano. Mediante un análisis exhaustivo de la normativa vigente, casos judiciales relevantes y opiniones de expertos en el campo, se pretende

ofrecer una descripción detallada de la utilización de agentes encubiertos informáticos en el sistema de justicia penal ecuatoriano.

En esta investigación descriptiva se llevó a cabo un análisis documental de la legislación penal ecuatoriana, incluyendo el Código Orgánico Integral Penal y otras normativas relacionadas con la investigación de delitos informáticos. También se examinarán casos judiciales relevantes en los cuales se haya utilizado el agente encubierto informático como herramienta de investigación. Además, se realizaron entrevistas a expertos en derecho penal y delitos informáticos en Ecuador, con el fin de recopilar opiniones y perspectivas sobre la viabilidad de esta técnica (Talavera, 2020).

1.3 Métodos y técnica de investigación

1.3.1 Métodos

La metodología utilizada en la investigación se corresponde a:

Analítico.

La metodología analítica asegurará la profundidad necesaria en la teoría cubierta, destacando el análisis de los datos recogidos de fuentes secundarias, apoyado en el procesamiento de datos sistemáticos, progresivos y lógicos de los que se derivarán las recomendaciones. Para lograr un análisis crítico y actualizado que sea efectivo y totalmente consistente con los objetivos de investigación anticipados, todas las observaciones realizadas durante la investigación deben reducirse a cero. (Bardales, 2021). El método analítico es una estrategia de investigación que se utiliza para descomponer y analizar los elementos y componentes de un fenómeno o problema. En el contexto del estudio de un Agente Encubierto Informático en el proceso penal ecuatoriano, el método analítico puede ser útil para examinar su viabilidad.

La viabilidad de utilizar un Agente Encubierto Informático en el proceso penal ecuatoriano se puede evaluar a través de un análisis detallado de la legislación y normativas vigentes en Ecuador. Esto implica examinar las leyes relacionadas con la investigación penal, el acceso a datos informáticos y la privacidad de las

comunicaciones electrónicas. El método analítico permitiría desglosar y comprender las disposiciones legales relevantes y evaluar si permiten o prohíben el uso de agentes encubiertos informáticos en el proceso penal (Talavera, 2020).

Además, el método analítico puede ayudar a evaluar la validez de la evidencia recopilada por un Agente Encubierto Informático. Esto implicaría descomponer y examinar los métodos utilizados por el agente para obtener pruebas, como la interceptación de comunicaciones electrónicas o la infiltración en sistemas informáticos. Se requeriría un análisis exhaustivo de las prácticas y técnicas utilizadas por el agente para determinar si cumplen con los estándares legales y constitucionales en Ecuador, así como si se respetaron los derechos fundamentales de los involucrados en la investigación.

Sintético

El método sintético se refiere a la combinación y síntesis de diversos elementos y fuentes de información para obtener una visión completa y holística de un fenómeno o problema. En el estudio de la viabilidad y validez del uso de un Agente Encubierto Informático en el proceso penal ecuatoriano, el método sintético puede ser valioso para obtener una comprensión global (Herbas & Rocha, 2018).

En este enfoque, se recopilan y analizan diferentes fuentes de información relevantes, como la legislación ecuatoriana, jurisprudencia, opiniones de expertos en derecho penal y tecnología, informes y estudios académicos, entre otros. Estas fuentes proporcionarán una variedad de perspectivas y enfoques que se pueden combinar y sintetizar para formar una imagen completa del tema en cuestión (Leyva et al., 2020).

Al aplicar el método sintético, se puede examinar cómo se ha abordado la cuestión del Agente Encubierto Informático en otros países con sistemas legales similares o comparables. Esto permitiría analizar cómo se han abordado los desafíos legales y éticos relacionados con este tipo de investigación en otros contextos, y si existen precedentes o directrices internacionales relevantes.

Inductivo

El método inductivo es un enfoque de investigación que se basa en la observación de casos particulares para llegar a conclusiones generales o principios. En el estudio de la viabilidad y validez del uso de un Agente Encubierto Informático en el proceso penal ecuatoriano, el método inductivo implica analizar casos concretos y extraer conclusiones a partir de ellos (Herbas & Rocha, 2018).

Para aplicar el método inductivo en este contexto, se pueden examinar casos pasados o actuales en los que se haya utilizado un Agente Encubierto Informático en investigaciones penales en Ecuador. Se analizarían los detalles de estos casos, como el contexto de la investigación, los delitos involucrados, las técnicas utilizadas por el agente encubierto y los resultados obtenidos. A partir de esta información, se podrían extraer conclusiones sobre la viabilidad del uso de agentes encubiertos informáticos en el proceso penal ecuatoriano.

Además, el método inductivo también puede implicar el análisis de estudios de casos similares en otros países con sistemas legales comparables. Esto permitiría identificar patrones o tendencias en el uso de agentes encubiertos informáticos y evaluar cómo se han resuelto las cuestiones legales y éticas relacionadas en esos casos (Leyva et al., 2020).

Es importante tener en cuenta que el método inductivo se basa en la recopilación y análisis riguroso de datos y casos relevantes. Por lo tanto, es necesario contar con una base de datos confiable de casos y un análisis cuidadoso de cada situación para evitar conclusiones precipitadas o sesgadas. El uso del método inductivo en el estudio de la viabilidad y validez del uso de un Agente Encubierto Informático en el proceso penal ecuatoriano puede proporcionar una base empírica sólida para comprender mejor las implicaciones legales y prácticas de este tipo de investigación en el contexto específico de Ecuador. Sin embargo, es importante complementar este enfoque con otros métodos de investigación y tener en cuenta el marco legal y normativo vigente en Ecuador (Herbas & Rocha, 2018).

Deductivo

El método deductivo es un enfoque de investigación que se basa en la aplicación de principios generales para llegar a conclusiones específicas. En el estudio de la viabilidad del uso de un Agente Encubierto Informático en el proceso penal ecuatoriano, el método deductivo implica utilizar leyes, normativas y principios legales existentes para analizar y evaluar la viabilidad y validez de este tipo de investigación (Leyva et al., 2020).

Para aplicar el método deductivo en este contexto, se pueden examinar las leyes y normativas relevantes en Ecuador que regulan el proceso penal y la investigación criminal. Se analizarían disposiciones legales relacionadas con la investigación, el acceso a datos informáticos, la privacidad de las comunicaciones electrónicas y otros aspectos relevantes para determinar si permiten o prohíben el uso de agentes encubiertos informáticos en el proceso penal.

A partir de estos principios legales, se pueden extraer conclusiones específicas sobre la viabilidad y validez del uso de un Agente Encubierto Informático en el contexto del proceso penal ecuatoriano (Herbas & Rocha, 2018).Por ejemplo, si las leyes ecuatorianas prohíben específicamente el uso de agentes encubiertos informáticos en ciertos casos o establecen restricciones claras sobre su uso, se podría concluir que su viabilidad es limitada o nula en esos contextos.

Además, el método deductivo también implica la aplicación de principios legales generales y precedentes jurisprudenciales para evaluar la validez de la evidencia obtenida a través de un Agente Encubierto Informático. Se analizaría si los métodos utilizados por el agente cumplen con los estándares legales y constitucionales en Ecuador, si se respetaron los derechos fundamentales de los involucrados y si la evidencia obtenida es admisible en un tribunal.

Es importante tener en cuenta que el método deductivo se basa en la interpretación y aplicación de las leyes y principios legales existentes. Por lo tanto, es fundamental contar con un conocimiento profundo del marco legal ecuatoriano y consultar fuentes legales actualizadas para garantizar una aplicación precisa del

método deductivo en el estudio de la viabilidad y validez del uso de un Agente Encubierto Informático en el proceso penal ecuatoriano (Leyva et al., 2020).

Exegético jurídico

El método exegético jurídico se refiere a un enfoque interpretativo y analítico utilizado en el campo del derecho para comprender y aplicar las leyes y normativas existentes. En el estudio de la viabilidad y validez del uso de un Agente Encubierto Informático en el proceso penal ecuatoriano, el método exegético jurídico implica un análisis detallado de las disposiciones legales y su interpretación en el contexto específico (Talavera, 2020).

Para aplicar el método exegético jurídico en este contexto, se examinarán las leyes y normativas relevantes en Ecuador que regulan el proceso penal, la investigación criminal, la protección de datos y la privacidad de las comunicaciones electrónicas. Se realizaría una lectura cuidadosa y minuciosa de estas disposiciones legales, prestando atención a los términos y definiciones utilizados, así como a la intención y el espíritu de la legislación.

El análisis exegético implica interpretar y comprender el significado de las disposiciones legales y cómo se aplican al uso de un Agente Encubierto Informático en el proceso penal. Se pueden analizar argumentos legales a favor y en contra de este tipo de investigación, considerando la protección de los derechos fundamentales, la legalidad de los métodos utilizados y los límites impuestos por la legislación (Leyva et al., 2020).

Además, el método exegético jurídico puede implicar el estudio de la jurisprudencia relevante, es decir, las decisiones judiciales pasadas relacionadas con el uso de agentes encubiertos informáticos en el proceso penal. El análisis de casos precedentes y la forma en que los tribunales han interpretado y aplicado la legislación en casos similares pueden proporcionar orientación y perspectivas adicionales sobre la viabilidad y validez de este tipo de investigación en Ecuador.

Es importante tener en cuenta que el método exegético jurídico requiere un conocimiento profundo del sistema legal ecuatoriano y la capacidad de realizar un

análisis riguroso de las leyes y normativas aplicables. Además, es fundamental tener en cuenta la evolución y los cambios en la legislación y la jurisprudencia, ya que pueden tener un impacto significativo en la viabilidad del uso de un Agente Encubierto Informático en el proceso penal ecuatoriano.

1.4 Población

Para determinar los análisis del proyecto de investigación, se realizará entrevistas a 3 abogados especializados en seguridad informática sobre la viabilidad del agente encubierto informático y el rol que desempeñará dentro de la normativa ecuatoriana. Por otro lado, también se realizará entrevistas a 3 jueces de lo penal todos ellos ubicados en la ciudad de Guayaquil.

1.4.1 Técnicas e instrumentos para la recolección de datos

Entrevista semiestructurada: Las entrevistas semiestructuradas a expertos en ciberseguridad son una herramienta valiosa en la investigación cualitativa de diseño no experimental sobre la viabilidad del uso de un Agente Encubierto Informático en el proceso penal ecuatoriano. Estas entrevistas permiten recopilar información detallada y contextualizada de profesionales con experiencia y conocimientos en el campo de la ciberseguridad.

La entrevista permite identificar los desafíos éticos, legales y prácticos percibidos por los abogados en relación con el uso de un Agente Encubierto Informático. Estas preocupaciones pueden ser fundamentales para evaluar la viabilidad de este enfoque en el contexto penal ecuatoriano.

Los abogados entrevistados pueden proporcionar información sobre la efectividad y validez de la evidencia obtenida a través de un Agente Encubierto Informático. Sus opiniones pueden contribuir a la comprensión de cómo esta evidencia es valorada y utilizada en el sistema judicial ecuatoriano.

Por otra parte, los jueces de lo penal entrevistados pueden proporcionar información valiosa sobre la admisibilidad de la evidencia obtenida a través de un Agente Encubierto Informático. Su conocimiento y experiencia en la interpretación y

aplicación de la ley pueden ayudar a evaluar si la evidencia cumpliría con los requisitos legales para ser admitida en un juicio.

1.5 Validez y confiabilidad de los instrumentos

Los procedimientos se utilizan en la creación de una investigación con el objetivo de evaluar la consistencia del diseño de la estructura de los instrumentos de recolección que se utilizarán para la recolección y recopilación de la información requerida para la ejecución de una investigación (García, 2020).

1.6 Técnicas de procesamiento y análisis de datos

Las técnicas de procesamiento y análisis de datos son fundamentales para obtener información significativa y útil a partir de los datos recopilados en una investigación. Aquí hay algunas técnicas comunes utilizadas en el procesamiento y análisis de datos:

Codificación: En el caso de datos cualitativos, la codificación implica la asignación de categorías o etiquetas a segmentos de texto o respuestas para organizar y estructurar los datos. Esto ayuda a identificar temas, patrones y relaciones entre diferentes elementos en los datos (Reyes & Avello, 2021).

Categorización: La categorización consiste en agrupar los datos en categorías relevantes y significativas. Esto se puede hacer utilizando un sistema de categorías predefinido o mediante la creación de categorías emergentes durante el análisis. La categorización facilita la comprensión y el análisis de los datos (Morán et al., 2019).

Análisis de contenido: El análisis de contenido implica el examen sistemático y detallado de los datos para identificar temas, patrones y significados en el contenido. Puede realizarse a través de un enfoque deductivo (basado en teorías o marcos conceptuales preexistentes) o inductivo (dejando que los temas y patrones emerjan de los datos) (Reyes & Avello, 2021).

Análisis temático: El análisis temático implica identificar, analizar y reportar patrones y temas clave en los datos cualitativos. Esto puede implicar la identificación de categorías temáticas y subtemas, así como el examen de conexiones y relaciones entre los temas identificados (Reyes & Avello, 2021).

Análisis de redes: En el análisis de datos relacionales o de redes, se exploran las relaciones y conexiones entre diferentes elementos. Esto implica la visualización y el estudio de la estructura de la red, así como el análisis de las propiedades y características de los nodos y las conexiones en la red (Morán et al., 2019).

Análisis comparativo: En el análisis comparativo, se comparan los datos entre diferentes grupos o categorías para identificar similitudes y diferencias.

CAPÍTULO III

RESULTADOS

3.1 Entrevista realizada a jueces de lo penal

1. **¿Considera que el uso de Agentes encubiertos Informáticos es viable en el proceso penal ecuatoriano?**

Experto 1: Si, es viable actualmente se vive en una era digital el cual por medio del agente encubierto informático considero que es una nueva medida para erradicar la delincuencia organizada y los grupos delictivos.

Experto 2: Definitivamente estoy a favor de la implementación del agente encubierto informático, vivimos en un Estado de derechos que aboga por la seguridad del Ecuador, no debe quedarse observando como evoluciona el mundo a través de la tecnología, sino que debe ser participé e implementarlo a su favor con el fin de garantizar seguridad a los ciudadanos.

Experto 3: Considero que sí es viable siempre y cuando se limite las facultades de este rol. Es una pieza fundamental para la lucha contra la ciberdelincuencia.

2. **¿Cree que la legislación ecuatoriana actual proporciona suficiente orientación y salvaguardias para el uso de Agentes Encubiertos Informáticos en el proceso penal?**

Experto 1: Actualmente con la reforma de la Ley Orgánica Reformatoria a varios cuerpos legales para el fortalecimiento de las capacidades institucionales y la seguridad integral, no existe suficiente orientación, la ley debería ser limitada acerca del agente encubierto informático para evitar vulneración de los derechos.

Experto 2: Debería delimitarse las facultades otorgadas al agente encubierto informático, las atribuciones otorgadas sin una ley sancionadora pueden interferir en la justicia y ser utilizado para otros fines.

Experto 3: Considero que en la actualidad el agente encubierto informático presenta varias contradicciones dentro del marco legal ecuatoriano.

3. **¿Cree que la utilización de Agentes Encubiertos Informáticos pueda contribuir a una mejor detección y persecución de delitos informáticos en Ecuador?**

Experto 1: En mi opinión, considero que la implementación del agente encubierto informático si contribuye en la detección de delitos informáticos. La ley debería cumplir con el desarrollo de ir creando un ciberespacio seguro. Por tal motivo es importante que la normativa garantice, la eficacia al momento de la investigación de un delito y la nula impunidad del delincuente.

Experto 2: El agente encubierto informático responde a la necesaria actualización de métodos de investigación a las nuevas tecnologías. Ofrecerá varios avances significativos en la legislación ecuatoriana. Sin embargo, se debería realizar un amplio estudio sobre este nuevo rol y la debida capacitación al personal encargado de dichas operaciones encubiertas.

Experto 3: A mi criterio, debería de existir un equilibrio ya que ayudaría con la persecución de delitos informáticos pero el internet y los sistemas informáticos al ser muy amplios se podría vulnerar los derechos de un tercero. Por tal motivo considero que debería implementar, pero así mismo que se creen sanciones en casos de que el agente encubierto informático quiera abusar y sobrepasar los límites de las facultades otorgadas.

4. **¿Considera que el uso del agente encubierto informático vulnera los derechos de los presuntos delincuentes?**

Experto 1: Considero que en la actualidad es contradictorio el rol del agente encubierto informático, ya que al no existir un órgano regulador de dichas operaciones encubiertas podría vulnerarse los derechos de los presuntos delincuentes, es importante crear un departamento que lleve un control de las operaciones para evitar y prevenir futuros casos de abuso de poder.

Experto 2: En mi opinión, estamos en un escenario cambiante, de tal manera que el derecho debe evolucionar y adaptarse a los nuevos avances. El agente encubierto informático es fundamental para progresar. Es importante realizar un estudio y comparar las demás legislaciones e investigar casos internacionales para implementar esta figura, con el fin de poder combatir el crimen cibernético.

Experto 3: Esta nueva herramienta es necesaria para la investigación criminal virtual, si se realiza un estudio y se crea una ley el cual limite las facultades del agente encubierto informático se evitaría casos de vulneración de principios y derechos.

5. **¿Cree usted que es necesario que se cree una norma legal para regular el uso del agente encubierto informático en el proceso penal ecuatoriano?**

Experto 1: Si, es fundamental crear una norma que regule el uso del agente encubierto informático. En la actualidad existe un vacío legal dentro de la legislación ecuatoriana, al momento de realizar la reforma y estar implementando por primera vez en el país, este rol debería de tener sanciones y prohibiciones en caso de que exista abuso de funciones.

Experto 2: En el proceso penal ecuatoriano todo debe estar tipificado, por tal motivo es importante crear una norma que regule porque al momento que se vulnere algún derecho y no se encuentre tipificado no podrá ser sancionado.

Experto 3: Si, es necesario el agente encubierto informático ya ha sido implementado en otros países, el cual cuentan con una legislación más desarrollada. La vida ha ido evolucionando y con ellos el derecho también, es fundamental que se cree una norma con el fin de combatir la ciberdelincuencia.

3.2 Entrevista realizada abogados expertos en ciberseguridad

1. **¿Está familiarizado con el concepto del Agente Encubierto Informático en el ámbito del proceso penal?**

Experto 1: Sí, estoy completamente familiarizado con el concepto del Agente Encubierto Informático en el ámbito del proceso penal. Este concepto se refiere al uso de herramientas tecnológicas y agentes encubiertos para investigar y recolectar pruebas en casos relacionados con delitos informáticos. Estos agentes se infiltran en redes o entornos digitales para recopilar información crucial y desenmascarar a los delincuentes en línea.

Experto 2: Sí, como experto en ciberseguridad, estoy muy familiarizado con el concepto del Agente Encubierto Informático en el ámbito del proceso penal. Estos agentes desempeñan un papel fundamental en la lucha contra la delincuencia en línea, ya que utilizan técnicas especializadas para infiltrarse en entornos digitales y obtener pruebas necesarias para llevar a cabo investigaciones y enjuiciamientos exitosos en casos de ciberdelincuencia.

Experto 3: Definitivamente, como experto en ciberseguridad, estoy bien informado sobre el concepto del Agente Encubierto Informático en el contexto del proceso penal. Estos agentes son fundamentales para recopilar información y evidencia en delitos informáticos complejos. Su capacidad para operar de manera encubierta en entornos digitales les permite identificar a los delincuentes y obtener pruebas sólidas que puedan ser utilizadas en los procedimientos legales.

El Agente Encubierto Informático es un concepto importante en el ámbito del proceso penal, especialmente en la lucha contra la delincuencia en línea y los delitos informáticos. Se refiere al uso de herramientas tecnológicas y expertos en ciberseguridad que se infiltran en redes o entornos digitales de forma encubierta con el propósito de recopilar información y pruebas cruciales para investigar y enjuiciar a los delincuentes.

Estos agentes desempeñan un papel fundamental en la obtención de pruebas necesarias para llevar a cabo investigaciones exitosas en casos de ciberdelincuencia. Al operar de manera encubierta en entornos digitales, tienen la capacidad de identificar a los delincuentes y obtener evidencia sólida que puede ser utilizada en los procedimientos legales. Su experiencia en ciberseguridad les permite utilizar técnicas especializadas para obtener información de manera discreta y asegurar la confidencialidad de sus operaciones.

2. **¿Considera que el uso de Agentes Encubiertos Informáticos es viable en el proceso penal ecuatoriano? ¿Por qué?**

Experto 1: Sí, considero que el uso de Agentes Encubiertos Informáticos es viable en el proceso penal ecuatoriano. La delincuencia informática es un problema creciente en la era digital, y para combatirla de manera efectiva, es necesario utilizar herramientas y técnicas especializadas. Los Agentes Encubiertos Informáticos pueden desempeñar un papel crucial en la obtención de pruebas y en la identificación de los responsables de delitos informáticos. Su capacidad para infiltrarse en entornos digitales y recopilar información valiosa puede contribuir significativamente a la persecución exitosa de los delincuentes y a la protección de la sociedad.

Experto 2: Sí, creo firmemente que el uso de Agentes Encubiertos Informáticos es viable en el proceso penal ecuatoriano. La naturaleza sofisticada de los delitos informáticos exige enfoques innovadores para investigar y reunir pruebas sólidas. Estos agentes, al operar encubiertos en el ámbito digital, pueden obtener información valiosa y recopilar pruebas cruciales para apoyar las investigaciones y los procesos judiciales. Su capacidad para adaptarse a los entornos en línea y recopilar información sin levantar sospechas los convierte en una herramienta valiosa en la lucha contra los delitos informáticos en Ecuador.

Experto 3: Sin lugar a dudas, considero que el uso de Agentes Encubiertos Informáticos es perfectamente viable en el proceso penal ecuatoriano. Los delitos informáticos son cada vez más sofisticados y requieren un enfoque estratégico para combatir eficazmente. Estos agentes, al operar encubiertos en el ciberespacio, pueden obtener información clave, infiltrarse en redes criminales y recopilar pruebas esenciales para desmantelar grupos delictivos. Su capacidad para adaptarse a las complejidades del mundo digital y su conocimiento especializado en ciberseguridad los convierten en un recurso valioso para fortalecer la lucha contra los delitos informáticos en el contexto legal ecuatoriano.

Los expertos están de acuerdo en que el uso de Agentes Encubiertos Informáticos es viable y necesario en el proceso penal ecuatoriano. La delincuencia informática en la era digital representa un desafío creciente, y para combatirla de

manera efectiva, se requiere el uso de herramientas y técnicas especializadas. Los Agentes Encubiertos Informáticos desempeñan un papel crucial al infiltrarse en entornos digitales y recopilar información valiosa que puede contribuir significativamente a la identificación y persecución exitosa de los delincuentes informáticos. Su capacidad para operar encubiertos y adaptarse a los complejos entornos en línea los convierte en un recurso valioso en la lucha contra los delitos informáticos y en la protección de la sociedad ecuatoriana.

3. **¿Cuáles serían los posibles beneficios del uso de Agentes Encubiertos Informáticos en la lucha contra los delitos informáticos en Ecuador?**

Experto 1: El uso de Agentes Encubiertos Informáticos en la lucha contra los delitos informáticos en Ecuador puede ofrecer varios beneficios significativos. Estos agentes tienen la capacidad de infiltrarse en grupos delictivos en línea, lo que les permite obtener información privilegiada y recolectar pruebas sólidas. Esto puede conducir a una mayor detección y desmantelamiento de redes criminales, lo que a su vez contribuye a reducir la incidencia de delitos informáticos en el país. Además, estos agentes encubiertos pueden ayudar a identificar nuevas técnicas y tendencias utilizadas por los delincuentes, lo que permite a las autoridades mantenerse actualizadas y adaptar sus estrategias de prevención y persecución.

Experto 2: El uso de Agentes Encubiertos Informáticos en la lucha contra los delitos informáticos en Ecuador puede brindar una serie de beneficios sustanciales. Estos agentes tienen la capacidad de infiltrarse en foros, redes sociales y plataformas en línea donde se planifican y ejecutan actividades delictivas. Al obtener información privilegiada, pueden identificar y recopilar pruebas sólidas sobre los delincuentes y sus actividades ilícitas. Esto puede fortalecer los casos judiciales, aumentar las tasas de condena y enviar un mensaje disuasorio a los posibles infractores. Además, la presencia de Agentes Encubiertos Informáticos puede contribuir a la prevención de delitos informáticos al disuadir a los delincuentes y generar un mayor temor a ser descubiertos.

Experto 3: El uso de Agentes Encubiertos Informáticos en la lucha contra los delitos informáticos en Ecuador puede tener una serie de beneficios significativos. Estos agentes tienen la capacidad de infiltrarse en comunidades y grupos

cibernéticos relacionados con actividades delictivas en línea. Al hacerlo, pueden recopilar información valiosa sobre la estructura de las organizaciones criminales, sus métodos y sus integrantes. Esto puede ayudar a las autoridades a comprender mejor las dinámicas de los delitos informáticos y a desarrollar estrategias más efectivas para su prevención y persecución. Además, el uso de Agentes Encubiertos Informáticos puede permitir la identificación temprana de amenazas emergentes y el seguimiento de delincuentes en tiempo real, lo que aumenta las posibilidades de detección y captura exitosa de los responsables de delitos informáticos en Ecuador.

Los expertos destacan que el uso de Agentes Encubiertos Informáticos en la lucha contra los delitos informáticos en Ecuador ofrece diversos beneficios. Estos agentes tienen la capacidad de infiltrarse en grupos delictivos en línea, lo que les permite obtener información privilegiada y recolectar pruebas sólidas. Esto puede llevar al desmantelamiento de redes criminales y reducir la incidencia de delitos informáticos en el país. Además, su presencia puede disuadir a los delincuentes y ayudar a las autoridades a mantenerse actualizadas en cuanto a técnicas y tendencias utilizadas en ciberdelincuencia, lo que mejora las estrategias de prevención y persecución. El uso de Agentes Encubiertos Informáticos también fortalece los casos judiciales, aumenta las tasas de condena y contribuye a la prevención al generar temor entre los delincuentes potenciales. Su capacidad para infiltrarse en comunidades en línea y recopilar información valiosa ayuda a comprender mejor las dinámicas de los delitos informáticos y permite la identificación temprana de amenazas emergentes, aumentando las posibilidades de detección y captura exitosa de los delincuentes.

4. **¿Cuáles son los principales desafíos o preocupaciones asociados con el uso de Agentes Encubiertos Informáticos en el proceso penal?**

Experto 1: El uso de Agentes Encubiertos Informáticos en el proceso penal presenta algunos desafíos y preocupaciones importantes. Uno de los principales desafíos es garantizar que el uso de estos agentes se realice dentro de los límites legales y éticos, sin violar los derechos fundamentales de los individuos investigados. Existe la preocupación de que el uso encubierto de estos agentes

pueda conducir a la obtención de pruebas ilícitas o a la vulneración de la privacidad de las personas. Por lo tanto, es crucial establecer salvaguardias y controles adecuados para asegurar que su utilización se realice de manera proporcional y respetando los derechos individuales.

Experto 2: Uno de los principales desafíos asociados con el uso de Agentes Encubiertos Informáticos en el proceso penal es el riesgo de que se generen pruebas ilícitas o se cometan excesos en la obtención de información. Existe la preocupación de que estos agentes, al operar encubiertos en entornos digitales, puedan violar la privacidad de las personas y recopilar información que no está directamente relacionada con las investigaciones en curso. Es necesario establecer pautas claras y estrictas para garantizar que el uso de estos agentes se limite a los casos adecuados y se realice de manera ética y proporcional.

Experto 3: Uno de los principales desafíos y preocupaciones asociados con el uso de Agentes Encubiertos Informáticos en el proceso penal radica en la necesidad de establecer salvaguardias sólidas para proteger los derechos fundamentales de los presuntos delincuentes. El uso de estos agentes puede plantear interrogantes en términos de la legalidad y la proporcionalidad de las técnicas empleadas, así como la posible violación de la privacidad y la confidencialidad de las comunicaciones. Por lo tanto, es fundamental implementar regulaciones claras y estrictas que definan los límites y restricciones del uso de Agentes Encubiertos Informáticos, asegurando que se respeten los derechos constitucionales y se eviten abusos o malas prácticas en su utilización.

El uso de Agentes Encubiertos Informáticos en el proceso penal presenta desafíos y preocupaciones importantes. Uno de los principales desafíos es garantizar que su utilización se realice dentro de los límites legales y éticos, sin violar los derechos fundamentales de los individuos investigados. Existe la preocupación de que su operación encubierta pueda llevar a la obtención de pruebas ilícitas o a la vulneración de la privacidad de las personas. Por lo tanto, es necesario establecer salvaguardias y regulaciones claras para asegurar que su uso sea proporcional y respete los derechos individuales. Se deben establecer pautas y restricciones para evitar excesos en la obtención de información y asegurar que su

empleo se limite a casos adecuados y de manera ética. La protección de los derechos fundamentales de los presuntos delincuentes debe ser una preocupación primordial al utilizar a estos agentes en el proceso penal.

5. **¿Cuál es su opinión sobre la legislación ecuatoriana actual en términos de orientación y salvaguardias para el uso de Agentes Encubiertos Informáticos en el proceso penal? ¿Es suficiente o se requieren mejoras?**

Experto 1: En mi opinión, la legislación ecuatoriana actual en términos de orientación y salvaguardias para el uso de Agentes Encubiertos Informáticos en el proceso penal requiere mejoras. Si bien existen disposiciones legales que abordan el uso de Agentes Encubiertos en general, la legislación específica que regula su utilización en el ámbito de la ciberseguridad y los delitos informáticos puede ser limitada o insuficiente. Es necesario establecer pautas más claras y detalladas el cual definan los límites, los procedimientos y las garantías necesarias para proteger los derechos fundamentales de los individuos investigados y evitar abusos en el uso de estos agentes.

Experto 2: En general, considero que la legislación ecuatoriana actual en términos de orientación y salvaguardias para el uso de Agentes Encubiertos Informáticos en el proceso penal está en proceso de desarrollo. Si bien existen algunas disposiciones generales, como la Ley de Delitos Informáticos, que pueden proporcionar cierta orientación, aún se requiere una mayor claridad y detalle en relación con el uso de Agentes Encubiertos en el contexto de los delitos informáticos. Es fundamental que la legislación establezca salvaguardias sólidas para proteger los derechos de los individuos, como la privacidad y la integridad de las comunicaciones en línea, al tiempo que permita el uso efectivo de estos agentes en la investigación y persecución de delitos informáticos.

Experto 3: En mi opinión, la legislación ecuatoriana actual en términos de orientación y salvaguardias para el uso de Agentes Encubiertos Informáticos en el proceso penal requiere mejoras significativas. Aunque existen algunos marcos legales que pueden ser aplicables a ciertos aspectos del uso de estos agentes, la legislación específica y detallada sobre su implementación y las garantías

necesarias para proteger los derechos de los individuos investigados puede ser insuficiente. Se necesita una revisión y actualización de la legislación para abordar de manera adecuada los desafíos y preocupaciones relacionados con la utilización de Agentes Encubiertos Informáticos en el contexto de los delitos informáticos. Es necesario establecer claramente los límites legales, las salvaguardias y los mecanismos de supervisión para asegurar un equilibrio adecuado entre la lucha contra los delitos informáticos y la protección de los derechos individuales.

Los expertos están de acuerdo en que la legislación ecuatoriana actual en términos de orientación y salvaguardias para el uso de Agentes Encubiertos Informáticos en el proceso penal necesita mejoras. Aunque existen algunas disposiciones legales generales, la legislación específica y detallada que regula el uso de estos agentes en el contexto de los delitos informáticos puede ser limitada o insuficiente. Es esencial establecer pautas claras y detalladas que definan los límites, los procedimientos y las garantías necesarias para proteger los derechos fundamentales de los individuos investigados y evitar abusos en el uso de estos agentes. Se necesita una revisión y actualización de la legislación para abordar de manera adecuada los desafíos y preocupaciones relacionados con el uso de Agentes Encubiertos Informáticos en la lucha contra los delitos informáticos y garantizar un equilibrio entre la persecución efectiva de los delitos y la protección de los derechos individuales.

6. **¿Cree que el uso de Agentes Encubiertos Informáticos podría afectar negativamente los derechos de los presuntos delincuentes? ¿Qué salvaguardias legales serían necesarias para proteger los derechos fundamentales?**

Experto 1: El uso de Agentes Encubiertos Informáticos podría potencialmente afectar los derechos de los presuntos delincuentes si no se implementan las salvaguardias legales adecuadas. Existe la posibilidad de que la utilización encubierta de estos agentes pueda violar la privacidad, la confidencialidad de las comunicaciones y otros derechos fundamentales de los individuos investigados. Para proteger estos derechos, es esencial establecer salvaguardias legales sólidas. Algunas medidas que podrían ser necesarias incluyen

la obtención de órdenes judiciales previas, la proporcionalidad en la recolección de pruebas, la limitación del alcance y la duración de las operaciones encubiertas, y la obligación de informar a los individuos afectados una vez concluida la investigación. Además, es crucial garantizar una supervisión efectiva y un mecanismo de rendición de cuentas para evitar abusos y asegurar que el uso de estos agentes se realice dentro de los límites legales establecidos.

Experto 2: El uso de Agentes Encubiertos Informáticos plantea preocupaciones legítimas sobre la posible afectación de los derechos de los presuntos delincuentes. Si bien es importante llevar a cabo investigaciones efectivas y combatir los delitos informáticos, se deben implementar salvaguardias legales para proteger los derechos fundamentales de los individuos investigados. Esto incluye garantizar el respeto a la privacidad, la confidencialidad de las comunicaciones y otros derechos consagrados en la legislación nacional e internacional. Las salvaguardias legales necesarias podrían incluir la obtención de autorizaciones judiciales previas, la proporcionalidad en la recolección y uso de pruebas, la limitación del tiempo y alcance de las operaciones encubiertas, así como el establecimiento de mecanismos de supervisión y rendición de cuentas para asegurar que el uso de estos agentes se realice dentro de los límites legales establecidos.

Experto 3: Es crucial reconocer que el uso de Agentes Encubiertos Informáticos tiene el potencial de afectar los derechos de los presuntos delincuentes. Para proteger los derechos fundamentales de los individuos investigados, se deben establecer salvaguardias legales adecuadas. Estas salvaguardias podrían incluir la necesidad de obtener autorizaciones judiciales para utilizar a estos agentes, la proporcionalidad en la recolección de pruebas, la limitación del alcance y duración de las operaciones encubiertas, y la garantía de que las acciones realizadas sean necesarias y proporcionadas para el caso en cuestión. Asimismo, es importante asegurar la confidencialidad de la información obtenida y establecer mecanismos de supervisión y control para prevenir abusos y garantizar que el uso de estos agentes se realice en conformidad con el marco legal y los estándares de derechos humanos aplicables.

Los expertos concuerdan en que el uso de Agentes Encubiertos Informáticos puede afectar los derechos de los presuntos delincuentes y que se requieren salvaguardias legales sólidas para proteger estos derechos. Es esencial establecer medidas como obtener autorizaciones judiciales previas, garantizar la proporcionalidad en la recolección de pruebas y limitar el alcance y la duración de las operaciones encubiertas. Además, se deben implementar mecanismos de supervisión y rendición de cuentas para asegurar que el uso de estos agentes se realice dentro de los límites legales establecidos y respetando los derechos fundamentales de los individuos investigados. La confidencialidad de la información obtenida y el cumplimiento de los estándares de derechos humanos también deben ser considerados en el uso de Agentes Encubiertos Informáticos.

7. **¿Cuál sería su recomendación para mejorar la regulación y el uso de Agentes Encubiertos Informáticos en el proceso penal ecuatoriano?**

Experto 1: Mi recomendación para mejorar la regulación y el uso de Agentes Encubiertos Informáticos en el proceso penal ecuatoriano sería establecer pautas claras y detalladas que definan los límites y las salvaguardias necesarias para proteger los derechos fundamentales de los individuos investigados. Estas pautas deberían incluir requisitos rigurosos para obtener autorizaciones judiciales previas, garantizar la proporcionalidad en la recolección y uso de pruebas, limitar el tiempo y alcance de las operaciones encubiertas, y establecer mecanismos sólidos de supervisión y rendición de cuentas. Además, sería beneficioso contar con un organismo independiente encargado de evaluar y supervisar la implementación de estas pautas, asegurando que se cumplan los estándares legales y éticos en el uso de estos agentes en el proceso penal.

Experto 2: Una recomendación importante para mejorar la regulación y el uso de Agentes Encubiertos Informáticos en el proceso penal ecuatoriano sería llevar a cabo una revisión exhaustiva de la legislación existente y actualizarla para abordar de manera adecuada los desafíos y preocupaciones actuales en el ámbito de los delitos informáticos. Esto debería incluir la promulgación de leyes específicas y detalladas que regulen el uso de Agentes Encubiertos Informáticos, estableciendo salvaguardias claras para proteger los derechos de los individuos investigados.

Además, sería recomendable capacitar adecuadamente a los jueces, fiscales y agentes encargados de utilizar a estos agentes, para asegurar su correcta aplicación y garantizar el respeto a los derechos fundamentales en todo momento.

Experto 3: Para mejorar la regulación y el uso de Agentes Encubiertos Informáticos en el proceso penal ecuatoriano, sería necesario promover una reforma legislativa que aborde específicamente las preocupaciones y desafíos asociados con estos agentes en el ámbito de los delitos informáticos. Esta reforma debería incluir la creación de una legislación clara y completa que establezca los límites, los procedimientos y las salvaguardias necesarias para garantizar el respeto a los derechos fundamentales de los individuos investigados. Además, se debería fomentar la cooperación y el intercambio de buenas prácticas con otros países que han implementado regulaciones efectivas en este campo. Asimismo, sería valioso fomentar el diálogo y la participación de expertos en ciberseguridad, abogados y organizaciones de derechos humanos en el proceso de diseño y revisión de la regulación, para asegurar que se tengan en cuenta diferentes perspectivas y se alcance un equilibrio adecuado entre la lucha contra los delitos informáticos y la protección de los derechos individuales.

Los expertos coinciden en que mejorar la regulación y el uso de Agentes Encubiertos Informáticos en el proceso penal ecuatoriano requiere acciones específicas. Estas recomendaciones incluyen establecer pautas claras y detalladas que defina los límites y salvaguardias para proteger los derechos de los individuos investigados. Esto podría lograrse mediante la obtención de autorizaciones judiciales previas, garantizando la proporcionalidad en la recolección y uso de pruebas, y limitando el tiempo y alcance de las operaciones encubiertas. Además, se sugiere la creación de leyes específicas para regular el uso de estos agentes en el contexto de los delitos informáticos y capacitar adecuadamente a los profesionales involucrados en su aplicación. La cooperación internacional y la participación de expertos y organizaciones de derechos humanos también se consideran esenciales para promover una regulación efectiva y equilibrada en este campo.

8. **¿Considera que el Agente Encubierto Informático puede desempeñar un papel importante en la lucha contra los delitos informáticos en el contexto ecuatoriano? ¿Por qué?**

Experto 1: Sí, considero que el Agente Encubierto Informático puede desempeñar un papel importante en la lucha contra los delitos informáticos en el contexto ecuatoriano. Los delitos informáticos son cada vez más sofisticados y difíciles de detectar, y es necesario utilizar herramientas y enfoques innovadores para combatirlos. Los Agentes Encubiertos Informáticos tienen la capacidad de infiltrarse en grupos delictivos en línea, recopilar información valiosa y obtener pruebas sólidas que pueden ser utilizadas en los procesos judiciales. Su conocimiento especializado en ciberseguridad y su capacidad para adaptarse a los entornos digitales les permiten identificar las técnicas y tendencias emergentes utilizadas por los delincuentes en Ecuador. Esto contribuye significativamente a mejorar la detección y persecución de los delitos informáticos en el país.

Experto 2: Definitivamente, considero que el Agente Encubierto Informático puede desempeñar un papel crucial en la lucha contra los delitos informáticos en el contexto ecuatoriano. La naturaleza de estos delitos requiere enfoques especializados y adaptados a las complejidades del mundo digital. Los Agentes Encubiertos Informáticos, al operar encubiertos en línea, tienen la capacidad de recopilar información sobre actividades delictivas, infiltrarse en grupos y redes criminales, y obtener pruebas sólidas para apoyar los procesos judiciales. Su presencia y acciones encubiertas pueden ser fundamentales para identificar y desmantelar organizaciones criminales, así como para prevenir futuros delitos informáticos al disuadir a los delincuentes potenciales.

Experto 3: Sí, considero que el Agente Encubierto Informático puede desempeñar un papel de gran relevancia en la lucha contra los delitos informáticos en Ecuador. La ciberdelincuencia es una amenaza en constante evolución y requiere respuestas efectivas y adaptadas a la realidad digital. Los Agentes Encubiertos Informáticos tienen la capacidad de infiltrarse en grupos delictivos en línea, recopilar información vital y desmantelar redes criminales que operan en el ámbito digital. Su conocimiento especializado y habilidades técnicas les permiten

identificar y recopilar pruebas sólidas, lo que fortalece los casos judiciales y contribuye a una persecución exitosa de los delincuentes informáticos. Además, su presencia encubierta en línea puede actuar como una medida disuasoria efectiva para prevenir futuros delitos informáticos al aumentar el riesgo y la incertidumbre para los delincuentes.

Los expertos coinciden en que el Agente Encubierto Informático puede desempeñar un papel importante y crucial en la lucha contra los delitos informáticos en Ecuador. Estos agentes tienen la capacidad de infiltrarse en grupos delictivos en línea, recopilar información valiosa y obtener pruebas sólidas que pueden ser utilizadas en los procesos judiciales. Su conocimiento especializado en ciberseguridad y habilidades técnicas les permiten identificar técnicas y tendencias emergentes utilizadas por los delincuentes, lo que mejora la detección y persecución de los delitos informáticos en el país. Además, su presencia encubierta en línea actúa como una medida disuasoria efectiva para prevenir futuros delitos informáticos.

3.3 Discusión de los resultados

Los resultados de las entrevistas realizadas a los jueces de lo penal, ofrecen una visión interesante sobre la viabilidad del uso del Agente Encubierto Informático, la mayoría de los jueces considera que es viable en el proceso penal ecuatoriano. Sin embargo, consideran que la legislación ecuatoriana no proporciona suficiente orientación para su uso. Estos resultados destacan la necesidad de revisar y mejorar la legislación existente para evitar abusos y garantizar el cumplimento de los derechos.

Según los datos proporcionados, una gran mayoría de los expertos en ciber seguridad entrevistados consideran que el uso de Agentes Encubiertos Informáticos es viable y válido en el proceso penal ecuatoriano. Esto sugiere que existe una percepción generalizada de que estos agentes pueden ser eficaces para la detección y persecución de delitos informáticos.

Los abogados que ven la viabilidad de los Agentes Encubiertos Informáticos destacan su capacidad para mejorar la detección y persecución de delitos

informáticos en Ecuador. Estos agentes pueden ser herramientas valiosas para recopilar pruebas en línea, identificar a los delincuentes y prevenir futuros delitos.

Sin embargo, algunos abogados expresan preocupaciones sobre el uso de estos agentes. Algunos de ellos consideran que la legislación ecuatoriana actual no proporciona suficiente orientación y salvaguardias para proteger los derechos de los presuntos delincuentes. También se menciona la corrupción y la complacencia de los funcionarios legales como posibles limitantes para el uso efectivo y ético de los Agentes Encubiertos Informáticos.

Otro punto a considerar es la discusión sobre la necesidad de crear normas y regulaciones específicas para el uso de Agentes Encubiertos Informáticos en el proceso penal ecuatoriano. Algunos abogados consideran que estas regulaciones adicionales podrían proporcionar orientación y salvaguardias claras para garantizar un uso adecuado y respetuoso de estos agentes.

En general, los resultados de las entrevistas reflejan la necesidad de un equilibrio entre la lucha contra los delitos informáticos y la protección de los derechos individuales en el contexto del uso de Agentes Encubiertos Informáticos en el proceso penal ecuatoriano. Estos resultados pueden servir como base para futuras discusiones y revisiones legislativas que busquen mejorar la regulación y el uso de estos agentes, teniendo en cuenta las preocupaciones planteadas por los jueces y abogados encuestados.

Si bien una gran mayoría de los abogados entrevistados consideran viable y válido el uso de estos agentes para mejorar la detección y persecución de delitos informáticos, es importante tener en cuenta las preocupaciones expresadas por algunos abogados en relación con la falta de orientación y salvaguardias adecuadas en la legislación actual. Estas preocupaciones destacan la importancia de establecer regulaciones claras que protejan los derechos de los presuntos delincuentes y eviten el abuso o la violación de los mismos.

Además, la mención de la corrupción y la complacencia de los funcionarios legales como posibles limitantes para el uso efectivo y ético de los Agentes Encubiertos Informáticos resalta la necesidad de abordar estos problemas dentro

del sistema legal. Esto podría implicar medidas adicionales, como auditorías y controles internos, para garantizar la integridad y la imparcialidad en el uso de estos agentes.

En definitiva, los resultados de las entrevistas proporcionan una visión general de las opiniones y preocupaciones de los abogados en relación con el uso de Agentes Encubiertos Informáticos en el proceso penal ecuatoriano. Estos resultados pueden servir como base para futuras discusiones y revisiones legislativas que busquen mejorar la regulación y el uso de estos agentes, tomando en consideración las perspectivas y preocupaciones planteadas por los profesionales del derecho.

CAPÍTULO IV

PROPUESTA

4.1 Presentación

La transformación digital global que se ha venido experimentando en las últimas décadas ha resultado en la aparición de nuevas formas de delincuencia. Dentro de este contexto, el cibercrimen ha cobrado relevancia y requiere una respuesta adaptada a los desafíos que plantea. En respuesta a este escenario, la legislación ecuatoriana ha implementado el Reglamento de Ley para la Aplicación del Agente Encubierto Informático. Esta herramienta legal se ha establecido como un medio para enfrentar y combatir eficazmente los delitos cibernéticos.

El agente encubierto informático se presenta como una figura única dentro de la legislación ecuatoriana, estableciendo un marco legal para que las autoridades puedan llevar a cabo investigaciones online de manera encubierta. Este mecanismo busca adaptar las estrategias de investigación a las nuevas formas de delincuencia y facilitar la recopilación de evidencia electrónica, una tarea que suele presentar diversos retos técnicos y legales.

La implementación del agente encubierto informático viene acompañada de un riguroso control y regulación. Es imperativo que se respeten los derechos fundamentales de los individuos, como la privacidad y la presunción de inocencia, durante todo el proceso de investigación. Asegurar este equilibrio entre la eficacia de la investigación y el respeto de los derechos es uno de los desafíos más significativos de la Ley.

El agente encubierto informático se emplea bajo ciertos criterios y condiciones, entre las que se incluyen la proporcionalidad, la necesidad y la legalidad. Las autoridades deben justificar su uso y demostrar que es la opción más adecuada para la investigación en cuestión. Además, la actuación de este agente se limita a ciertos delitos graves, como la explotación sexual infantil online, el ciberterrorismo y el fraude informático, entre otros.

La figura del agente encubierto informático en la legislación ecuatoriana responde a la necesidad de adaptarse a un mundo cada vez más digitalizado, en el que los delitos cibernéticos presentan retos importantes. La Ley para su Aplicación es un paso positivo en esta dirección, estableciendo un marco legal claro y regulado para su uso.

Sin embargo, es vital que se mantenga una revisión constante y una adaptación continua del marco legal a los avances tecnológicos y a las nuevas formas de delincuencia. Además, el respeto a los derechos fundamentales debe ser siempre una prioridad, y la actuación del agente encubierto informático debe estar sujeta a rigurosos controles y equilibrios.

La Ley es un hito significativo en la lucha contra el cibercrimen en Ecuador, y representa un modelo a seguir para otros países que buscan abordar de manera efectiva este tipo de delincuencia. Es un ejemplo del compromiso del país con la protección de su ciudadanía en la era digital, y una muestra de su voluntad para adaptarse a los desafíos que este nuevo contexto presenta.

Es importante señalar que la aplicación efectiva de la Ley requiere no sólo un marco legal sólido, sino también la formación adecuada de las autoridades encargadas de implementar esta nueva figura. La naturaleza técnica y en constante cambio del cibercrimen exige que los agentes encubiertos informáticos estén equipados con el conocimiento y las habilidades necesarias para navegar y operar de manera efectiva en el entorno digital.

El trabajo conjunto entre los sectores legal, tecnológico y de seguridad es fundamental para la formación de estos profesionales. El intercambio de conocimientos y experiencias entre estos sectores permitirá no solo una mejor aplicación de la Ley, sino también su continua adaptación y mejora en función de los desafíos que se presenten.

Por otro lado, también es crucial la cooperación internacional en este campo. El cibercrimen no conoce fronteras y, por lo tanto, requiere un esfuerzo global para combatirlo. Ecuador, con la implementación de esta Ley, muestra su compromiso

con la lucha global contra el cibercrimen y abre la puerta a la cooperación y el intercambio de mejores prácticas con otros países.

La Ley para la Aplicación del Agente Encubierto Informático en la legislación ecuatoriana es una respuesta necesaria y adecuada a la creciente amenaza del cibercrimen. Su éxito no solo dependerá de la solidez del marco legal y el respeto a los derechos fundamentales, sino también de la preparación de los agentes encubiertos, la cooperación intersectorial e internacional, y la capacidad para adaptarse a los cambios y desafíos futuros del entorno digital.

4.2 Objetivos

4.2.1 Objetivo general

El objetivo general de la Ley para la Aplicación del Agente Encubierto Informático en la Legislación Ecuatoriana es combatir y prevenir el cibercrimen, a través del establecimiento de un marco legal sólido y coherente que permita a las autoridades utilizar la figura del agente encubierto informático en el ámbito de las investigaciones de delitos cometidos en el entorno digital.

4.2.2 Objetivos específicos

- Adaptar la legislación a las nuevas formas de delincuencia: La aparición de los delitos cibernéticos ha generado la necesidad de adaptar las estrategias de investigación y las leyes existentes a este nuevo contexto. La implementación de la figura del agente encubierto informático es una respuesta a esta necesidad.
- Establecer un marco legal para la actuación de los agentes encubiertos informáticos: La Ley proporciona directrices claras y estrictas sobre cómo, cuándo y bajo qué circunstancias los agentes encubiertos informáticos pueden operar, asegurando su uso apropiado y eficaz.
- Asegurar el respeto a los derechos fundamentales: A pesar de la necesidad de investigar y combatir el cibercrimen, es crucial garantizar que los derechos fundamentales, como la privacidad y la presunción de inocencia, se respeten. La Ley establece controles y salvaguardias para este fin.

- Facilitar la recopilación de evidencia digital: La recolección de pruebas en el entorno digital puede ser un desafío debido a su naturaleza volátil y a la complejidad técnica. La figura del agente encubierto informático busca facilitar esta tarea y proporcionar medios más eficaces para obtener pruebas.
- Fomentar la cooperación entre diferentes organismos y entidades: El combate al cibercrimen requiere de la colaboración entre diversas instituciones, tanto a nivel nacional como internacional. La Ley promueve la cooperación y coordinación entre los organismos de seguridad, los operadores de telecomunicaciones y los proveedores de servicios de Internet.
- Establecer penas proporcionales y disuasorias para los ciberdelincuentes: Uno de los objetivos de la Ley es asegurar que aquellos que cometan delitos cibernéticos enfrenten sanciones adecuadas y disuasorias, proporcionando así un fuerte incentivo para disuadir la comisión de tales delitos.

4.3 Justificación de la propuesta de Ley para la Aplicación del Agente Encubierto Informático en la Legislación Ecuatoriana

El mundo digital, caracterizado por su constante evolución y crecimiento, ha generado desafíos significativos para la seguridad y la justicia. Entre ellos, el cibercrimen ha emergido como una amenaza real que requiere medidas proactivas y adaptadas. Ante esto, la legislación ecuatoriana ha propuesto la Ley para la Aplicación del Agente Encubierto Informático.

El avance tecnológico ha remodelado la vida en sociedad y, paralelamente, ha dado origen a nuevas formas de delincuencia. La ciberdelincuencia, que abarca desde fraudes informáticos hasta delitos más graves como el ciberterrorismo o la explotación infantil online, ha demostrado la necesidad de adaptar nuestra legislación a la realidad digital. En este sentido, la propuesta de la Ley para la Aplicación del Agente Encubierto Informático es un paso crucial para abordar estos desafíos.

La figura del agente encubierto informático permite a las autoridades investigar delitos en el entorno digital de manera más efectiva y eficiente. Los agentes pueden operar en el entorno virtual sin revelar su identidad, permitiéndoles acceder a redes de cibercriminales y recoger evidencia clave para las

investigaciones. Este método de operación es especialmente útil dada la naturaleza global y a menudo anónima del cibercrimen.

No obstante, la implementación de estos agentes no puede realizarse sin un marco legal sólido que regule su actuación y garantice el respeto de los derechos fundamentales de las personas. La propuesta de Ley se justifica también en la necesidad de mantener un equilibrio entre la lucha eficaz contra el cibercrimen y la protección de los derechos como la privacidad y la presunción de inocencia.

Además, la propuesta de Ley facilita la cooperación y coordinación interinstitucional en el combate al cibercrimen. Al establecer normas claras y procedimientos específicos, la Ley propicia un marco de colaboración más efectivo entre las autoridades judiciales, las fuerzas de seguridad, los proveedores de servicios de Internet y otros actores relevantes.

La propuesta de Ley para la Aplicación del Agente Encubierto Informático en la legislación ecuatoriana se justifica en su necesidad de adaptarse a la realidad digital, su potencial para mejorar la eficacia de las investigaciones de cibercrimen, la importancia de proteger los derechos fundamentales en el entorno digital y la promoción de la cooperación interinstitucional. Con su aprobación, Ecuador estará dando un paso significativo en la lucha contra el cibercrimen, posicionándose como un país comprometido con la seguridad y justicia en la era digital.

Al mismo tiempo, es crucial entender que esta Ley no es una solución aislada. Debe ser parte de un enfoque más amplio y holístico para combatir el cibercrimen que también incluya la educación y la concienciación del público, la creación de infraestructuras de seguridad cibernética sólidas y la promoción de normas de comportamiento ético en el ciberespacio.

Además, la naturaleza internacional del cibercrimen requiere una respuesta global. La propuesta de Ley también enfatiza la importancia de la cooperación internacional en la lucha contra el cibercrimen. Ecuador, con esta iniciativa, puede servir como ejemplo para otros países y liderar esfuerzos de colaboración en la región y en el mundo. La actualización constante de la Ley será necesaria dada la evolución rápida y continua de la tecnología y los métodos de cibercrimen. Es

esencial que el marco legal pueda adaptarse y responder a estos cambios para seguir siendo efectivo.

Finalmente, la protección de los derechos fundamentales es una responsabilidad que no debe tomarse a la ligera. La Ley propuesta incluye medidas para asegurar que el uso de agentes encubiertos informáticos se realice de manera proporcional y necesaria, y que se mantenga el respeto a la privacidad y otros derechos.

En conclusión, la propuesta de Ley para la Aplicación del Agente Encubierto Informático en la legislación ecuatoriana es una iniciativa esencial y justificada para combatir el creciente problema del cibercrimen. Al equilibrar la necesidad de eficacia en la lucha contra el cibercrimen con la protección de los derechos fundamentales, Ecuador se posiciona como un líder en la protección de su ciudadanía en la era digital.

4.4 Modelo operativo de la propuesta de Ley para la Aplicación del Agente Encubierto Informático en la Legislación Ecuatoriana

El modelo operativo de la propuesta de Ley para la Aplicación del Agente Encubierto Informático en la Legislación Ecuatoriana está diseñado para ser una herramienta efectiva y flexible en la lucha contra el cibercrimen, proporcionando a las autoridades los medios necesarios para enfrentar esta amenaza moderna. No obstante, se hace hincapié en un enfoque equilibrado que prioriza tanto la seguridad pública como el respeto de los derechos fundamentales de los ciudadanos.

Actuación del Agente Encubierto Informático: El agente encubierto informático tiene la facultad de operar en internet, simulando una identidad falsa o asumiendo un perfil que le permita infiltrarse en comunidades o redes donde se sospecha que se cometen delitos cibernéticos. Sin embargo, la actuación de este agente está sujeta a ciertas limitaciones, sólo pudiendo intervenir en casos de delitos graves como ciberterrorismo, explotación sexual infantil, fraude informático y otros delitos que comprometan la seguridad del Estado.

Autorización Judicial: El uso del agente encubierto informático no es discrecional, requiere de una autorización judicial previa para iniciar sus operaciones. Para ello, las autoridades competentes deben presentar suficiente evidencia que justifique la necesidad de la intervención y demostrar que se han agotado o son ineficaces otros métodos de investigación.

Proporcionalidad, Necesidad y Legalidad: Estos tres principios guían la actuación del agente encubierto informático. Las actividades llevadas a cabo deben ser proporcionales a la gravedad del delito investigado, necesarias para la resolución del caso, y siempre dentro de los límites de la ley.

Recolección y Preservación de Evidencia Digital: El agente encubierto informático también tiene la responsabilidad de recoger y preservar la evidencia digital en el proceso de la investigación. Las evidencias recolectadas deben ser manejadas con el mayor cuidado para mantener su integridad y utilidad en futuros procesos judiciales.

Respeto a los Derechos Fundamentales: La Ley enfatiza la protección de los derechos fundamentales, incluso en el contexto de investigaciones de cibercrimen. El respeto a la privacidad y la presunción de inocencia son pilares fundamentales que deben ser respetados en todo momento. La Ley prevé mecanismos de control y revisión para evitar cualquier abuso de poder o violación de estos derechos.

Cooperación Interinstitucional e Internacional: La efectividad de la Ley depende en gran medida de la cooperación tanto a nivel interinstitucional como internacional. La naturaleza transfronteriza del cibercrimen requiere esfuerzos de colaboración a escala global para su prevención, detección y persecución.

Actualización y Adaptabilidad: El marco legal debe ser adaptable a las rápidas transformaciones y evoluciones del ciberespacio. Por lo tanto, se requiere una revisión y actualización constante de la Ley para mantener su relevancia y eficacia.

El modelo operativo propuesto se centra en maximizar la eficacia en la lucha contra el cibercrimen, al tiempo que se asegura el respeto de los derechos fundamentales y se mantiene la adaptabilidad en un ambiente digital en constante cambio. La Ley para la Aplicación del Agente Encubierto Informático, por lo tanto, se posiciona como un componente clave en el marco jurídico ecuatoriano para enfrentar los desafíos de la era digital.

4.5 Propuesta de Ley para la Aplicación del Agente Encubierto Informático en la Legislación Ecuatoriana

ASAMBLEA NACIONAL

COMISIÓN LEGISLATIVA Y DE FISCALIZACIÓN

EL PLENO DE LA COMISIÓN LEGISLATIVA Y DE FISCALIZACIÓN

Considerando:

Que: El Artículo 66 Garantiza una serie de derechos que pueden ser relevantes para la operación de un agente encubierto informático, incluyendo el derecho a la intimidad y a la inviolabilidad del domicilio y de la correspondencia, y el derecho a la protección de datos personales.

Que: Artículo 77. Establece principios generales para el proceso penal, como la presunción de inocencia y el derecho a la defensa.

Que: Artículo 78. Prohíbe el uso de pruebas obtenidas violando los derechos constitucionales, lo que podría ser relevante en caso de que un agente encubierto informático obtenga pruebas de manera inapropiada

Que: Artículo 120 enumera las funciones de la Asamblea Nacional, entre las que se encuentra la facultad de "crear, modificar, interpretar y derogar las leyes y reformar la Constitución". Esta es la base constitucional que permite a la Asamblea Nacional redactar y aprobar leyes, incluyendo potencialmente una ley que regule el uso de agentes encubiertos informáticos.

Que: El Artículo 133 detalla el procedimiento para la aprobación de leyes y resoluciones, y el Artículo 138 establece el procedimiento de veto y objeción presidencial a las leyes aprobadas por la Asamblea.

En ejercicio de las facultades establecidas en el artículo 120, numeral 6 de la Constitución de la República, expide la siguiente

LEY PARA LA APLICACIÓN DEL AGENTE ENCUBIERTO INFORMÁTICO EN LA LEGISLACIÓN ECUATORIANA

ARTÍCULO 1: DISPOSICIONES GENERALES

Objeto: Esta Ley tiene por objeto establecer el marco legal para la utilización de agentes encubiertos informáticos en la investigación de delitos cibernéticos.

Ámbito de aplicación: Esta Ley será de aplicación a todas las autoridades competentes encargadas de la investigación de delitos cibernéticos.

ARTÍCULO 2: DEL AGENTE ENCUBIERTO INFORMÁTICO

Definición: Se entenderá por agente encubierto informático a la persona autorizada para actuar en el ciberespacio de manera encubierta en el marco de una investigación criminal.

Actuación: El agente encubierto informático actuará exclusivamente en los casos en que se investiguen delitos cibernéticos graves.

ARTÍCULO 3: DE LA AUTORIZACIÓN JUDICIAL

Solicitud: Las autoridades competentes deberán solicitar la autorización judicial para utilizar un agente encubierto informático, debiendo justificar la necesidad, proporcionalidad y legalidad de dicha medida.

La utilización del agente encubierto informático deberá ser autorizada por una autoridad competente, previa solicitud fundamentada por parte de la entidad encargada de la investigación del delito cibernético.

La autorización deberá contener la descripción detallada de la investigación, los delitos que se pretenden investigar, los medios tecnológicos y digitales que serán utilizados y los plazos de duración de la operación encubierta.

La autorización deberá ser revisada y renovada periódicamente, de acuerdo a la complejidad y duración de la investigación, así como los avances y resultados obtenidos hasta el momento.

Resolución: El juez competente emitirá una resolución motivada, autorizando o denegando la utilización del agente encubierto informático.

ARTÍCULO 4: DEL PROCEDIMIENTO

Recolección de información: El agente encubierto informático recogerá información relevante para la investigación, siempre respetando los principios de necesidad, proporcionalidad y legalidad.

Preservación de evidencia: El agente encubierto informático deberá asegurarse de que la evidencia recopilada sea preservada y mantenida íntegra para su eventual uso en procesos judiciales.

ARTÍCULO 5: LIMITACIONES Y PROHIBICIONES DEL AGENTE ENCUBIERTO INFORMÁTICO

El agente encubierto informático no podrá inducir a la comisión de delitos, excepto cuando sea estrictamente necesario para obtener pruebas o prevenir delitos más graves.

El agente encubierto informático no podrá exceder los límites establecidos en la autorización, ni utilizar los medios tecnológicos y digitales de forma indiscriminada o fuera del marco legal.

El agente encubierto informático no podrá revelar su identidad ni poner en riesgo la seguridad de terceros involucrados en la investigación.

ARTÍCULO 6: SUPERVISIÓN Y CONTROL DE LAS OPERACIONES ENCUBIERTAS

Las operaciones encubiertas llevadas a cabo por el agente encubierto informático estarán sujetas a un estricto control y supervisión por parte de las autoridades competentes.

Las operaciones encubiertas informáticas serán bajo la supervisión de la fiscalía general del Estado y procederán los delitos, tales como:

a) Delitos de obtención, tráfico ilícito de órganos humanos.
b) Delitos de secuestro de personas, trata de personas.
c) Pornografía con utilización de niñas, niños y adolescentes.
d) Delitos de tráfico de armas, municiones o explosivos.
e) Delitos de terrorismo.
f) Delincuencia organizada y delitos relacionados.
g) Delitos relativos a la propiedad intelectual.
h) Tráfico de hidrocarburos y demás delitos que sean en contra de la eficiente administración pública.

Se establecerá un mecanismo de informes y registros detallados de las actuaciones del agente encubierto informático, que deberán ser presentados ante las autoridades competentes periódicamente.

ARTÍCULO 7: DE LA PROTECCIÓN DE DERECHOS FUNDAMENTALES

Respeto a los derechos: En todas las actuaciones del agente encubierto informático se respetarán los derechos fundamentales de las personas, incluyendo el derecho a la privacidad y la presunción de inocencia.

Durante el desarrollo de las operaciones encubiertas, se garantizará en todo momento el respeto a los derechos fundamentales de las personas, incluyendo el derecho a la privacidad, la inviolabilidad del domicilio y la protección de los datos personales.

La obtención y utilización de información obtenida por el agente encubierto informático deberá estar sujeta a las normas de protección de datos personales establecidas por la legislación ecuatoriana.

ARTÍCULO 8: DE LA COLABORACIÓN INTERINSTITUCIONAL E INTERNACIONAL

Cooperación: Se promoverá la cooperación y coordinación con otros entes nacionales e internacionales para una mayor efectividad en la lucha contra el cibercrimen.

Se promoverá la cooperación internacional en la lucha contra la delincuencia cibernética, incluyendo el intercambio de información y la colaboración en investigaciones que involucren a agentes encubiertos informáticos.

La cooperación internacional deberá realizarse de acuerdo a los tratados, convenios y acuerdos suscritos por Ecuador, respetando los principios de reciprocidad, confidencialidad y respeto a los derechos humanos.

ARTÍCULO 9: RESPONSABILIDAD Y SANCIONES

El agente encubierto informático será responsable de sus actuaciones y estará sujeto a las sanciones establecidas por la legislación ecuatoriana en caso de incumplimiento de sus obligaciones y prohibiciones.

Las autoridades competentes deberán realizar una revisión periódica de las operaciones encubiertas y evaluar su impacto, así como la legalidad y proporcionalidad de las actuaciones del agente encubierto informático.

ARTÍCULO 10: DE LA REVISIÓN Y ACTUALIZACIÓN

Adaptabilidad: Se establecerán mecanismos para la revisión y actualización constante de la Ley, con el fin de adaptarse a las evoluciones del ciberespacio y los avances tecnológicos.

DISPOSICIÓN FINAL:

Vigencia: La ley entrará en vigencia a partir de su publicación en el Registro Oficial y deberá ser aplicada de manera coordinada con la legislación vigente que rige la investigación y persecución de delitos informáticos en Ecuador.

Dado en San Francisco de Quito, a los 27 de julio del 2024.

_____ _____

Presidente secretario

CONCLUSIONES

Tras analizar la legislación ecuatoriana vigente en relación al agente encubierto informático, se puede concluir que Ecuador está tomando medidas significativas para adaptar su sistema jurídico a los desafíos planteados por la era digital. El reconocimiento de la necesidad de implementar un marco legal para los agentes encubiertos informáticos por primera vez en la normativa ecuatoriana, demuestra una comprensión clara de los retos contemporáneos del cibercrimen.

En cuanto a la situación actual de la aplicación del agente encubierto informático en la legislación ecuatoriana, se puede diagnosticar que si bien existen esfuerzos para su implementación, la falta de un marco legal sólido y bien definido ha generado algunos desafíos en términos de eficacia de las investigaciones y respeto a los derechos fundamentales. Existe la necesidad de un marco regulador que equilibre entre la lucha eficaz contra el cibercrimen y la protección de los derechos fundamentales, como la privacidad y la presunción de inocencia.

Al desarrollar una ley para la aplicación del agente encubierto informático en la legislación ecuatoriana, se debe considerar la proporcionalidad, necesidad y legalidad de la medida. Es fundamental que la ley establezca claramente los criterios y condiciones bajo los cuales puede operar un agente encubierto, los tipos de delitos en los que puede intervenir, y los procedimientos para la recolección y preservación de evidencia electrónica.

Por lo antes expuesto, es evidente que, al comparar otra normativa con la legislación ecuatoriana sobre el agente encubierto informático, existe un gran vacío legal en cuanto a tu temporalidad y facultades asignadas, es decir, al no tener una limitación y no estar tipificado se puede llegar a vulnerar derechos. Por lo tanto, su ámbito de actuación deberá ser reducido sólo aquellos tipos penales designados y utilizar este rol como último recurso.

El desarrollo de la ley es un paso vital para enfrentar de manera eficiente el cibercrimen. Esta normativa permitirá a las autoridades emplear métodos de investigación adaptados al entorno digital y proporcionará las garantías necesarias para respetar los derechos fundamentales de los individuos.

Esta legislación también fomentará la cooperación y colaboración interinstitucional, estableciendo una base sólida para la acción conjunta entre diferentes entidades en la lucha contra el cibercrimen. Además, se espera que facilite la recopilación y el intercambio de información relevante para las investigaciones, fortaleciendo de esta manera la capacidad de respuesta del país frente a estos delitos.

Aunque la ley representa un avance significativo, es fundamental recordar la necesidad de una revisión y actualización constantes para mantener su relevancia en un mundo digital en constante evolución. La tecnología y las formas de delincuencia en línea no dejan de cambiar, por lo que es esencial que la legislación y los métodos de investigación sigan el ritmo de estos cambios.

Además, la implementación de la ley deberá ser acompañada de medidas de transparencia y rendición de cuentas. La sociedad debe poder confiar en que los agentes encubiertos informáticos están trabajando para su protección y no en su contra, la confianza pública en estas medidas es esencial para su éxito.

El desarrollo de la ley es un paso importante hacia una legislación ecuatoriana más preparada y adaptada a los desafíos que plantea el cibercrimen. Sin embargo, su implementación y revisión deben hacerse con cuidado y diligencia, siempre teniendo en cuenta la necesidad de equilibrar la eficacia de la investigación con el respeto a los derechos fundamentales y la confianza del público.

Finalmente, es importante destacar que la implementación de un agente encubierto informático en la legislación ecuatoriana deberá estar acompañada de una revisión y actualización constante. El dinamismo del ciberespacio y los rápidos avances tecnológicos exigen que la legislación sea flexible y adaptable a los cambios que se produzcan en el futuro.

Con la implementación de la Ley para la Aplicación del Agente Encubierto Informático, Ecuador se posiciona en la vanguardia de la lucha contra el cibercrimen, proporcionando un modelo que puede ser de interés para otros países en el desarrollo de su propio marco legal para enfrentar este tipo de delincuencia. La ley no solo establece un método eficiente y adaptado a la realidad digital para la

investigación de delitos, sino que también resalta la importancia del equilibrio entre la seguridad y los derechos fundamentales, como la privacidad y la presunción de inocencia. Es una demostración de cómo se puede utilizar la tecnología y la innovación legislativa para abordar los desafíos contemporáneos sin dejar de proteger las libertades individuales.

Además, al fomentar la cooperación y coordinación interinstitucional, la Ley pone de manifiesto la importancia de un enfoque unificado para combatir el cibercrimen, haciendo hincapié en que la lucha contra estas nuevas formas de delincuencia requiere el esfuerzo conjunto de diversas entidades y sectores.

Sin embargo, al seguir el ejemplo de Ecuador, otros países deberán tener en cuenta que la aplicación de estas medidas del agente encubierto informático, es viable dentro del marco normativo, siempre y cuando se lleve un riguroso control y supervisión, con el fin de evitar cualquier abuso o violación de derechos. También es crucial recordar que cualquier marco legal que se desarrolle debe ser lo suficientemente flexible para adaptarse a la rápida evolución de la tecnología y de las formas de cibercrimen.

RECOMENDACIONES

Respecto al análisis de la legislación ecuatoriana vigente en relación al agente encubierto informático, se recomienda llevar a cabo un estudio exhaustivo que permita identificar posibles áreas de mejora, tales como la definición precisa del papel del agente encubierto informático, los derechos y deberes que le incumben, y las condiciones y limitaciones para su aplicación.

Además, es fundamental evaluar cómo se han venido implementando estas disposiciones en la práctica, para entender cuáles han sido las principales dificultades y logros obtenidos. Este análisis debería incluir también una revisión de las decisiones judiciales relevantes y de cómo se ha interpretado y aplicado la ley en diferentes casos.

En lo que respecta a la situación actual de la aplicación del agente encubierto informático en la legislación ecuatoriana, es importante hacer un diagnóstico que permita evaluar el alcance real y la efectividad de esta figura legal. Se debe analizar, por ejemplo, la cantidad y tipo de delitos que se han investigado gracias a su aplicación, los resultados obtenidos y los retos enfrentados.

Para desarrollar la ley para la aplicación del agente encubierto informático, es imprescindible contar con un marco legal claro y específico que regule minuciosamente su funcionamiento, respetando siempre los derechos fundamentales de los ciudadanos. Este reglamento debe establecer los criterios de aplicación, las responsabilidades y obligaciones del agente, así como los mecanismos de supervisión y control para garantizar su correcta aplicación.

Es vital mantener una revisión constante de este marco legal, para poder adaptarlo de forma continua a las nuevas formas de cibercrimen y a los avances tecnológicos. El cibercrimen es un fenómeno en constante evolución, y por ello es necesario que la legislación también evolucione para poder hacerle frente de manera eficaz.

Al diagnosticar la situación actual de la aplicación del agente encubierto informático en la legislación ecuatoriana, se recomienda recoger datos empíricos el cual reflejen cómo se ha utilizado esta figura hasta el momento. La información obtenida puede ser valiosa para identificar oportunidades de mejora en su aplicación y evaluar la eficacia de este mecanismo.

Es importante entender el alcance de la utilización de agentes encubiertos informáticos en términos de tipos de delitos cibernéticos abordados, el número de investigaciones realizadas, la cantidad y calidad de la evidencia recopilada y el impacto que estos han tenido en los procesos judiciales y en las tasas de condena. Igualmente, es relevante recoger datos sobre la formación y preparación que se les brinda a estos agentes y su adaptabilidad a los cambios tecnológicos.

Este diagnóstico permite, además, analizar si el marco legal existente proporciona suficientes salvaguardias para los derechos fundamentales de los individuos, y si existen suficientes mecanismos de control y supervisión para prevenir posibles abusos en la utilización de estos agentes.

Al desarrollar la ley para la aplicación del agente encubierto informático, es fundamental involucrar a todas las partes interesadas en el proceso, incluyendo a la judicatura, a las fuerzas de seguridad, a los proveedores de servicios de Internet y a la sociedad civil. Esto permitirá recoger un amplio rango de perspectivas y garantizar que la ley sea equilibrada y adecuada.

Se recomienda que la ley incluya disposiciones claras y específicas en relación a la protección de los derechos fundamentales durante la aplicación del agente encubierto informático. Es crucial que se establezcan mecanismos de control y supervisión para prevenir cualquier abuso o mal uso de esta herramienta.

En el desarrollo de la ley, se considera la creación de programas de formación y actualización para los agentes encubiertos informáticos. La naturaleza en constante cambio del ciberespacio y las tecnologías de la información requiere que estos profesionales estén al día en las últimas tendencias y técnicas.

Se recomienda que la universidad Ecotec dé a conocer el presente proyecto de investigación del agente encubierto informático a la Asamblea Nacional para implementar lo anteriormente expuesto con el fin de limitar las facultades del rol del agente encubierto y poder combatir el crimen organizado.

Por otra parte, este tipo de operaciones encubiertas informáticas deberían tener un mayor control, la fiscalía general del Estado debe ser el encargado de capacitar al personal y crear un departamento específicamente que lleve estos casos con el fin de evitar que se vulneren los derechos de los ciudadanos, llevando un control. Se debería utilizar este procedimiento como última instancia, es decir, en los casos que ya no exista otra forma de investigarlos. Aplicación de última ratio.

Finalmente, se recomienda que la legislación ecuatoriana vigente sea revisada y actualizada periódicamente para asegurar que sigue siendo relevante y eficaz en la lucha contra el cibercrimen. Esta revisión debería considerar los desarrollos tecnológicos, las tendencias del cibercrimen y las buenas prácticas internacionales en este ámbito.

La tecnología y las formas de cibercrimen evolucionan rápidamente y es fundamental que la ley sea capaz de mantenerse al día con estos cambios. Esto implica adaptar y modificar la normativa para abordar nuevas formas de delincuencia, mejorar la formación y preparación de los agentes encubiertos informáticos y garantizar su eficacia en el uso de las nuevas herramientas y tecnologías.

Asimismo, la revisión de la legislación debe considerar las tendencias emergentes en el cibercrimen para identificar áreas que requieran un enfoque más enfático. También es importante analizar y aprender de las buenas prácticas internacionales en esta área, lo que puede permitir a Ecuador mejorar su propio marco legal y sus prácticas de investigación y enjuiciamiento de delitos cibernéticos.

REFERENCIAS

Acosta, D. (2022). *Exclusión de responsabilidad penal del agente encubierto: Estudio de un caso* [MasterThesis, Quito, EC: Universidad Andina Simón Bolívar, Sede Ecuador]. http://repositorio.uasb.edu.ec/handle/10644/8966

Alcalá, L. (2021). El principio constitucional de publicidad procesal y el derecho a la información. *Cuadernos Constitucionales*, *2*, Article 2. https://doi.org/10.7203/cc.2.22764

Arevalo, J., & Rojas, J. (2021). *Procedimiento idóneo para la intervención de dispositivos móviles de agente encubierto informático en la recolección de material probatorio a la legislación Colombiana*. http://repository.unilibre.edu.co/handle/10901/20603

Asamblea Nacional del Ecuador. (2008). *Constitución de la República del Ecuador*. https://www.oas.org/juridico/pdfs/mesicic4_ecu_const.pdf

Asencio, E. (2022). *Exención de responsabilidad penal del agente encubierto por su acción provocadora en los delitos de tracto sucesivo (tráfico ilícito de drogas)*. http://tesis.usat.edu.pe/handle/20.500.12423/4770

Aveiga, M., Espinoza, D., & Ocampo, A. (2021). El principio de la constitucionalización del proceso penal en el sistema procesal penal acusatorio del Ecuador. *Revista Mapa*, *5*(22), Article 22. https://revistamapa.org/index.php/es/article/view/272

Bravo, C. (2021). *El agente encubierto en línea: Principales características, derecho comparado, y desafíos que subyacen a su regulación*. https://repositorio.uchile.cl/handle/2250/180210

Carrillo, Y. (2021). *Riesgos, afectaciones de los derechos fundamentales y vacíos legales existentes en la figura legal del agente encubierto previsto en el código procesal penal vigente, como mecanismo real y práctico para combatir la delincuencia en nuestra sociedad*. http://repositorio.unprg.edu.pe/handle/20.500.12893/9746

Caycho, J., & Saguma, D. (2021). MEDIDAS DE PROTECCIÓN INFORMÁTICA Y SU EFICACIA EN LA PREVENCIÓN DEL DELITO DE SUPLANTACIÓN DE IDENTIDAD CIBERNETICA EN LA CIUDAD DE TRUJILLO, 2020. *Universidad Privada de Trujillo*. http://181.176.219.234/handle/UPRIT/421

Cutire, J. (2023). *Lavado de activos y el crimen organizado bajo la percepción de los operadores de justicia de Lima Sur 2022*. http://repositorio.ulasamericas.edu.pe/xmlui/handle/123456789/3733

Cutrona, S. (2023). *Drogas, política y actores sociales en la Argentina democrática*. EUDEBA.

Cuyares, S. (2019). *Agente encubierto: Retos de legalidad, eficacia y respeto a los derechos fundamentales*. http://repository.unimilitar.edu.co/handle/10654/34955

Fuentes, E. (2022). *El derecho fundamental a la protección de datos personales en Argentina y en el mundo: Los conflictos extraterritoriales por los delitos informáticos*. http://repositorio.udesa.edu.ar/jspui/handle/10908/22383

García, S. (2021). *Método para la prevención y mitigación de vulnerabilidades en redes WI-FI.* http://repository.unad.edu.co/handle/10596/44590

Guamán, C. (2023). *Estudio jurídico del artículo 190 del código orgánico integral penal sobre la apropiación fraudulenta por medios electrónicos en la provincia de Imbabura* [Thesis, Pontificia Universidad Católica del Ecuador Ibarra]. https://doi.org/10/948

Guix, A. (2022). *Las diligencias de investigación y la prueba electrónica del cibercrimen*.

Hernández, C. (2021). *La ciberdelincuencia transnacional. Principales desafíos en la investigación durante pandemia por Covid-19*.

Hernández, S. (2019). *El agente encubierto: Especial atención al agente encubierto informático*. https://riull.ull.es/xmlui/handle/915/16410

Jácome, O. (2019). *Impacto de la aplicación del código orgánico integral penal en la incidencia de la violencia y la delincuencia* [B.S. thesis]. Guayaquil: ULVR, 2019.

León, A. (2021). *El agente encubierto y los derechos fundamentales en el marco del proceso penal garantista en el Perú*.

López, T. (2023). *LAS NUEVAS DILIGENCIAS DE INVESTIGACIÓN ELECTRÓNICAS*.

Manayalle, K. (2023). *Inoperatividad del agente especial para realizar labores de infiltración al interior de organizaciones criminales Chiclayo 2019*. http://repositorio.unprg.edu.pe/handle/20.500.12893/11306

Montalbano, L. (2019). *El reglamento europeo de protección de datos personales y el derecho al olvido*.

Morinelly, J. (2021). *Actuación del agente encubierto virtual como técnica especial de investigación criminal*. http://repository.unilibre.edu.co/handle/10901/20495

Moyano, C. (2021). *Online Grooming: Estudio del delito en la ciudad de Rosario* [B.S. thesis]. Facultad de Ciencia Política y Relaciones Internacionales.

Pino, P. del. (2019). *Las videoconferencias en Audiencias de Juicio Penal Derecho a la Defensa y Principio de Inmediación* [BachelorThesis, Quito: UCE]. http://www.dspace.uce.edu.ec/handle/25000/20627

Ramos, I. (2021). XXXII Seminario Internacional de Defensa—Amenazas desde el ciberespacio. *Descripcion: http://www.apeuropeos.org/xxxii-seminario-internacional-de-seguridad-y-defensa-amenazas-desde-el-ciberespacio/ Volumen: 32 Pagina Inicio: 159 Pagina Fin: 165*. https://repositorio.comillas.edu/xmlui/handle/11531/55854

Rodríguez, M. (2021). *Empleo de bots y agentes encubiertos para la detección del ciberacoso y su valor probatorio*. https://repositorio.uchile.cl/handle/2250/182330

Rojas, V. (2023). Incluir en el delito de Trata de Personas a la Explotación Reproductiva de mujeres, adolescentes y niñas, a quienes en contra de su voluntad se les practica técnicas de reproducción humana asistida, obligándolas a la procreación de niños. *Universidad Nacional Mayor de San Marcos*. https://cybertesis.unmsm.edu.pe/handle/20.500.12672/19602

Rúa, M. (2023). *Cibercriminalidad e investigación penal tecnológica: Una mirada desde la experiencia de la Cooperación Internacional para la persecución de la cibercriminalidad en Latinoamérica*. Palestra Editores.

Segovia, M. (2022). *La averiguación del delito a través de las medidas de investigación tecnológica*. https://repositori.uji.es/xmlui/handle/10234/198123

Vinueza, L. (2021). *Estudio técnico y normativo en el ámbito de las telecomunicaciones respecto a la evolución de la cantidad de equipos móviles reportados como robados, perdidos o hurtados en el Ecuador durante los años 2014 a 2018* [MasterThesis, PUCE - Quito]. http://repositorio.puce.edu.ec:80/handle/22000/18677