Revista Perspectivas Sociales y Administrativas

https://perspectivas.esprint.tech

Vol. 3 N° 1, enero-junio 2025 (85-97)

ISSN: 3028-8983

Artículo de revisión

La metodología utilizada por el agente encubierto informático en la recopilación de pruebas en delitos cibernéticos y el derecho a la intimidad de terceras personas

The methodology used by the undercover cyber agent in the collection of evidence in cybercrimes and the right to privacy of third parties

Jhonatan Daniel Almeida Mancheno*
Universidad Nacional de Chimborazo
Riobamba - Ecuador
jhonatan.almeida@unach.edu.ec
https://orcid.org/0009-0000-7686-0742

Jorge Marcelo Quintana Yánez
Fiscalía General del Estado
Ambato - Ecuador
marcelo.quintana.y@gmail.com
https://orcid.org/0009-0002-8666-378X

***Correspondencia:**
jhonatan.almeida@unach.edu.ec

Cómo citar este artículo:
Almeida, J., & Quintana, J. (2025). La metodología utilizada por el agente encubierto informático en la recopilación de pruebas en delitos cibernéticos y el derecho a la intimidad de terceras personas. *Perspectivas Sociales y Administrativas*, *3*(1), 85-97. https://doi.org/10.61347/psa.v3i1.79

Recibido: *2 de mayo de 2025*
Proceso de evaluación:
3 de mayo al 4 de junio de 2025
Aceptado: *6 de junio de 2025*
Publicado: *18 de junio de 2025*

Resumen: La metodología utilizada por el agente encubierto informático en la recopilación de pruebas resulta un tema controversial, debido al alcance e información que obtenga por la naturaleza de su trabajo. Dentro del ejercicio de sus funciones, el agente puede tener acceso a fotos y vídeos explícitos de terceras personas ajenas al proceso, lo cual violenta directamente el derecho constitucional de intimidad. Por tal razón, la presente investigación establece mediante un análisis jurídico, doctrinario y crítico cómo la metodología utilizada por el agente encubierto informático en la recopilación de pruebas en delitos cibernéticos violenta el derecho constitucional a la intimidad, con el fin de promover limitaciones a las actuaciones de dichos investigadores. Se realizó un análisis teórico basado en el Código Orgánico Integral Penal, la Constitución de la República del Ecuador, investigaciones e informes sobre la temática objeto de esta investigación. Como resultado se obtuvo un análisis académico confiable respecto a la implicancia de una incorrecta metodología del agente encubierto informático, y cómo violenta el derecho constitucional a la intimidad de terceras personas ajenas a la investigación penal.

Palabras clave: Agente encubierto informático, delitos cibernéticos, derecho a la intimidad, metodología.

Abstract: *The methodology used by the undercover computer agent in the collection of evidence is a controversial issue, due to the scope and information obtained by the nature of his work. In the course of his duties, the agent may have access to explicit photos and videos of third parties outside the process, which directly violates the constitutional right to privacy. For this reason, this research establishes through a legal, doctrinal and critical analysis how the methodology used by the undercover computer agent in the collection of evidence in cybercrimes violates the constitutional right to privacy, to promote limitations to the actions of such investigators. A theoretical analysis was carried out based on the Organic Integral Penal Code, the Constitution of the Republic of Ecuador, research and reports on the subject matter of this research. As a result, a reliable academic analysis was obtained regarding the implications of an incorrect methodology of the undercover computer agent, and how it violates the constitutional right to privacy of third parties outside the criminal investigation.*

Keywords: *Computer undercover agent, cybercrime, methodology, right to privacy.*

1. Introducción

En el marco del derecho penal, los elementos de convicción tanto de cargo como de descargo que se recolecten en el tiempo de la investigación previa y la instrucción fiscal resultan vitales para el resultado de un proceso penal. En una etapa de juicio, pueden llevar al juez al convencimiento de los hechos imputados sobre una persona, o a mantener la duda razonable. En consecuencia, debe escogerse una metodología para la obtención de pruebas que apoye legalmente una sentencia condenatoria o ratificatoria de inocencia.

No se discute la relevancia de la prueba dentro de un proceso penal: si una de las partes tiene la razón, pero no la puede probar es como si no la tuviera, de ahí proviene la importancia de la obtención de elementos que respalden lo alegado. El derecho de las partes a probar sus argumentos dentro de un caso en materia penal es el aspecto más significativo dentro del derecho procesal penal (Bravo, 2010).

La prueba, para el esclarecimiento de los hechos resulta, además, el elemento central del proceso judicial en cualquier rama del derecho y en el ámbito penal. No obstante, la forma en que esta es obtenida resulta determinante para establecer su validez. Si la prueba ha sido recolectada vulnerando derechos fundamentales reconocidos en la Constitución de la República del Ecuador (2008) carece de validez y eficacia dentro del proceso. Según el artículo 76 las pruebas obtenidas con violación de la ley o de la Constitución no serán tomadas en cuenta por la o el juzgador, al estar afectadas de nulidad.

La metodología empleada por un agente encubierto debe estar previamente autorizada por la ley y por las autoridades competentes. Según el Manual de Técnicas de Investigación Agente Encubierto y Técnica Vigilada (Oficina de las Naciones Unidas contra la Droga y el Delito, 2013), corresponde a la autoridad jurisdiccional competente, a requerimiento fundamentado del fiscal del caso, autorizar la intervención del agente encubierto mediante resolución. En el caso particular del agente encubierto informático, es fundamental considerar que, debido a la naturaleza de sus funciones, existe el riesgo de acceder a información de carácter personal e íntima, como fotografías o videos pertenecientes a terceras personas ajenas al proceso penal, lo que podría implicar una vulneración del derecho constitucional a la intimidad.

La presente investigación se centra en un tema de gran relevancia para Ecuador: la metodología utilizada por el agente encubierto informático en la recopilación de pruebas en delitos cibernéticos y el derecho a la intimidad de terceras personas. Para esta investigación se analizó la normativa que regula las actuaciones de los agentes encubiertos, llamado Código Orgánico Integral Penal (COIP), así como el aseguramiento de datos dentro del marco de una investigación.

Con los antecedentes expuestos, emerge la siguiente hipótesis: la falta de limitación en la metodología utilizada por el agente encubierto informático en la recopilación de pruebas en delitos cibernéticos afecta al derecho a la intimidad de terceras personas ajenas al proceso penal. De esta manera, el objetivo general consiste en establecer mediante un análisis jurídico, doctrinario y crítico cómo la metodología utilizada por el agente encubierto informático en la recopilación de pruebas en delitos cibernéticos puede violentar el derecho constitucional a la intimidad.

2. Metodología

Se asumió un enfoque cualitativo y se ejecutó un análisis teórico que facilitó el conocimiento general del tema en cuestión, a partir de lo establecido en la Constitución sobre el derecho a la intimidad; en el COIP (2014) sobre las actuaciones del agente encubierto; entre otros documentos rectores. La investigación correlacional permitió describir los fenómenos y establecer una relación de causalidad o explicar por qué ocurren ciertos eventos.

Para un mejor entendimiento de los materiales y la metodología utilizada, la tabla 1 expone los aspectos considerados para la selección de información utilizada en la presente investigación.

Tabla 1

Metodología

Aspecto	Explicación
Hipótesis	Esta investigación busca sustentar la siguiente hipótesis: La falta de limitación en la metodología utilizada por el agente encubierto informático en la recopilación de pruebas en delitos cibernéticos afecta al derecho a la intimidad de terceras personas cuando estas son ajenas al proceso penal. Área: agente encubierto informático, pruebas, derecho a la intimidad.
Estrategias de investigación	Propósito de la búsqueda: establecer mediante un análisis jurídico, doctrinario y crítico como la metodología utilizada por el agente encubierto informático en la recopilación de pruebas en delitos cibernéticos violenta el derecho constitucional a la intimidad, con el fin de promover limitaciones a las actuaciones de dichos investigadores.
Fuentes de información	Normas legales vigentes, jurisprudencia, artículos científicos, investigaciones.
Motores de búsqueda	Google académico.
Criterios de búsqueda	La limitación en la metodología de la recolección de pruebas del agente encubierto informático y la protección del derecho a la intimidad.
Criterios de inclusión	Documentos que contienen información sobre las actuaciones de los agentes encubiertos informáticos y el derecho a la intimidad. Documentos que contengan información sobre la metodología utilizada por los agentes encubiertos informáticos en la recolección de pruebas.
Análisis de la información	Se proporciona una visión general referente la forma como un agente encubierto informático recolecta pruebas, y cómo atenta contra el derecho a la intimidad de terceros ajenos al proceso penal
Criterio de especialistas	El presente análisis fue contrastado por dos abogados en libre ejercicio; el primer especialista en derecho penal con formación en la Universidad de Cuenca; el segundo especialista en criminalística con formación en la Universidad Integral del Caribe y América Latina (UNICAL).

3. Resultados

Rol y funciones del agente encubierto tradicional e informático en la normativa ecuatoriana

En la normativa penal ecuatoriana se establece que la fiscalía dirige la investigación preprocesal con la ayuda de agentes especializados que recolectan ciertos elementos para la evolución del proceso. Dentro de los agentes especializados se encuentran los encubiertos, quienes indagan en delitos que requieren mayor investigación para abrir un proceso penal.

Según Yánez (2017), el agente encubierto es un miembro de la Policía Nacional o de las Fuerzas Armadas que se introduce en una organización criminal utilizando una identidad ficticia, con el objetivo de conocer la preparación o comisión de delitos.

Este tipo de investigación constituye un instrumento esencial en la lucha contra la delincuencia organizada, siempre que se aplique conforme con la normativa correspondiente y bajo los principios de legalidad y proporcionalidad. En esta línea, Sandoval (2023) señala que un agente encubierto debe orientarse al conocimiento interno de la organización, con la finalidad de lograr su desarticulación total. Dado que el crimen organizado está presente a nivel global y se especializa en delitos de alta complejidad, esta técnica se vuelve necesaria para enfrentarlo desde sus estructuras fundamentales.

Dentro de las operaciones encubiertas, también se reconocen los agentes encubiertos informáticos, quienes han cobrado relevancia a partir del crecimiento de los delitos cibernéticos o ciberdelitos. Esta modalidad delictiva ha evolucionado significativamente, al punto de originar el Convenio de Budapest, aprobado por el Consejo de Europa y ratificado por más de 56 países, incluidos varios fuera del continente europeo. Montalbano (2019) afirma que dicho convenio promueve la cooperación internacional en la lucha contra los delitos informáticos cometidos en el ciberespacio. El agente encubierto informático, al igual que uno tradicional, se infiltra en grupos delictivos con el objetivo de recopilar información y evitar futuros ataques (Cevallos, 2023).

La justificación para la existencia 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. López & García-Erazo (2023) destacan que el uso de este tipo de agente permite investigar delitos informáticos, ciberdelitos, fraudes electrónicos, delitos contra la propiedad intelectual, entre otros, que se ejecutan mediante medios electrónicos o dentro del entorno digital.

El COIP establece que el fiscal puede autorizar al personal del Sistema Especializado Integral de Investigación de Medicina Legal y Ciencias Forenses para realizar tareas investigativas encubiertas mediante el uso de una identidad ficticia. Estas acciones incluyen patrullajes e intervenciones digitales en el ciberespacio, con el fin de infiltrarse en plataformas informáticas como foros, grupos de comunicación o espacios cerrados de información, para dar seguimiento a personas, vigilar objetos, efectuar compras controladas o esclarecer hechos delictivos vinculados con el uso o afectación de tecnologías de la información y comunicación, incluyendo ciberdelitos puros, réplicas u otros delitos relacionados.

En este contexto, el agente encubierto informático actúa en el entorno digital con el objetivo de recolectar evidencia que pueda convertirse en prueba dentro de un proceso penal. Por ello, resulta esencial conocer las metodologías y técnicas utilizadas para la obtención de dichas pruebas. Para Pazmiño (2023) esta labor debe basarse en una validación científica, que respalde teóricamente el procedimiento, y en una validación técnica, que garantice su operatividad y efectividad en la práctica.

Problemas éticos y legales derivados de la actuación del agente encubierto informático

En las operaciones encubiertas informáticas, el agente puede infiltrarse en el ciberespacio para realizar tareas de vigilancia. Según el COIP (art. 483.1), en el desarrollo de sus actividades, el agente encubierto puede obtener imágenes y realizar grabaciones en audio o video de las conversaciones que mantenga con los investigados, dependiendo de la naturaleza y modus operandi de la organización. No obstante, esta redacción ambigua no establece límites claros sobre el alcance de la vigilancia, lo que podría permitir que el agente actúe como un cibercriminal en un sentido amplio.

Sotomayor (2024) advierte que la ambigüedad normativa permite un uso discrecional y subjetivo de la figura del agente encubierto, lo que podría derivar en vigilancia masiva. Además, señala que dicha norma faculta al agente para anticiparse a conductas delictivas, lo cual contrasta con la naturaleza de los delitos cibernéticos, que generalmente son de resultado y no de tentativa. Estas infracciones suelen ser cometidas por ciberdelincuentes organizados que acceden ilegalmente a espacios digitales restringidos con fines patrimoniales o sexuales. Sin embargo, no todo hacker es un delincuente. Enríquez (2021) diferencia a los llamados hackers de sombrero blanco, quienes usan técnicas similares a las de los hackers maliciosos, pero con fines defensivos y siempre con autorización legal o del titular del sistema.

Investigar a grupos de ciberdelincuentes es una tarea compleja debido al carácter transnacional del internet y a las posibilidades de anonimato que ofrecen las herramientas antiforenses. En respuesta a esta problemática, se creó la figura del agente encubierto informático, cuya labor consiste en infiltrarse en redes delictivas, identificar infractores y evitar que los delitos se consumen o se agraven. Para ello, estos agentes emplean técnicas de hackeo como el phishing, ataques de fuerza bruta y malware, que les permiten vulnerar sistemas digitales y obtener información crucial para sustentar procesos penales. El agente que logra hackear una computadora o celular de los investigados puede encontrarse con fotos o vídeos de menores de edad, por lo que debe tener extremo cuidado en el tratamiento de este material audiovisual, con el fin de evitar que las víctimas de estos delitos sean revictimizadas si se llegan a difundir este contenido (Juca-Maldonado & Medina-Peña, 2023).

Hipotéticamente, un agente encubierto informático, como miembro especializado de la Policía Nacional, puede acceder a la vida privada de los investigados, lo que no solo implica una posible afectación a su intimidad, sino a la de terceros ajenos al proceso penal. Por ejemplo, si el investigado pertenece a una organización criminal dedicada a delitos sexuales cibernéticos, podría tener en su dispositivo contenido íntimo de su pareja o de personas que le enviaron voluntariamente imágenes o videos privados. Estas personas, sin ser parte procesal, ven comprometida su privacidad por la intervención del agente, lo que representa una transgresión a derechos constitucionales. La situación se vuelve aún más delicada cuando el agente no investiga delitos sexuales, sino otros informáticos como apropiación fraudulenta mediante medios electrónicos, revelación ilegal de bases de datos o intercepción de información. Este tipo de conductas están tipificadas y sancionadas por el artículo 190 del COIP (2014), el cual establece penas privativas de libertad para quienes manipulen sistemas o redes informáticas con fines ilícitos.

Las organizaciones delictivas cometen actividades ilícitas con fines de lucro, como la venta de información reservada, lo cual puede constituir espionaje y conlleva consecuencias jurídicas. En este contexto, el agente encubierto informático tiene la facultad de hackear los sistemas de estas organizaciones para identificar el tipo de infracciones que se cometen, incluso si no están relacionadas con delitos sexuales, como lo establece el artículo 190 del COIP. No obstante, durante el ejercicio de sus funciones puede encontrarse con contenido explícito o conversaciones privadas de personas ajenas a la investigación. Si bien las reformas al COIP autorizan ciertos ataques cibernéticos con fines investigativos, no se contempla adecuadamente la figura del hallazgo accidental, propia de la informática forense. El agente puede vulnerar un sistema, como un teléfono inteligente, sin conocer de antemano qué datos contiene, lo que podría derivar en la exposición de información sensible de terceros no vinculados al proceso, afectando así su derecho a la intimidad.

La Constitución en su Art. 66 reconoce y garantiza el derecho a la intimidad personal y familiar, que protege a las personas frente a cualquier intromisión en su vida privada. Villa & Calle (2023) lo definen como la facultad de excluir a otros del conocimiento de su esfera personal. En este contexto, dicho

derecho se ve comprometido cuando un agente encubierto informático accede a conversaciones o imágenes privadas de terceros no vinculados con el proceso, ya que les impide ejercer control sobre la reserva de su información, aun cuando esta haya sido compartida de forma confidencial.

El agente encubierto informático tiene facultad legal para vulnerar la privacidad de sospechosos o investigados cuando existen indicios de delito; sin embargo, esta autorización no debería extenderse a terceros ajenos a la investigación. Si durante su labor el agente accede accidentalmente a información privada de estas terceras personas, aunque inicialmente no incurre en delito debido a su autorización legal según lo previsto en el artículo 178 del COIP, sí podría ser sancionado conforme al artículo 179 de este mismo cuerpo legal en caso de divulgar dicha información personal o íntima a otros individuos. En definitiva, aunque el descubrimiento sea accidental, el solo acceso a información privada ya implica una vulneración del derecho constitucional a la intimidad, especialmente grave cuando afecta a personas no vinculadas con el proceso penal.

Propuestas de regulación y soluciones frente a los vacíos normativos existentes

No existe un reglamento que regule las actuaciones de estos agentes, lo que da luz verde a que se vulnere el derecho a la intimidad de terceras personas ajenas a la investigación penal. Resulta importante realizar una ponderación de derechos sobre cual pesa más: si el derecho a la intimidad o el derecho a la integridad económica o sexual de víctimas o futuras víctimas de los grupos delincuenciales cibernéticos.

Es necesario contemplar la creación de un reglamento de actuaciones de los agentes encubiertos informáticos, donde se limite sus actividades, funciones y participaciones dentro de una investigación preprocesal en contra de una persona o grupos delincuenciales encargados de realizar ciberdelitos. Es imposible erradicar completamente los descubrimientos accidentales por su carácter impredecible, pero se puede mermar mediante el uso de metodologías que detecten la posibilidad de encontrarse con contenido o información explícita dentro de una red privada o en medio electrónicos.

La Fiscalía General del Estado (2022) cuenta con el Reglamento para la Aplicación de las Entregas Vigiladas o Controladas que establece directrices claras sobre esta figura investigativa. En su artículo 8, literal c, se dispone que una entrega vigilada o controlada puede ser suspendida o finalizada cuando su ejecución vulnere o pueda vulnerar la Constitución, el ordenamiento jurídico interno o los derechos fundamentales. Esta disposición podría servir de base para la elaboración de un reglamento específico que regule las actuaciones de los agentes encubiertos informáticos.

En dicho reglamento se debería establecer que, previa autorización judicial y con una motivación debidamente fundamentada, el agente pueda suspender, rechazar o dar por terminada una operación de infiltración digital cuando existan indicios reales de que dicha intervención podría afectar la intimidad o privacidad de personas que no forman parte de la investigación penal. Esta medida permitiría equilibrar la necesidad de investigar delitos cibernéticos con la obligación de proteger los derechos fundamentales de terceros, fortaleciendo así la legalidad y legitimidad del accionar del sistema penal.

La tabla 2 presenta una sistematización de las respuestas brindadas por un abogado penalista respecto al papel de los agentes encubiertos informáticos en el contexto ecuatoriano. A través de preguntas clave, se recogió su visión sobre la pertinencia, legalidad y riesgos asociados con el uso de esta figura en las investigaciones preprocesales. En términos generales, el especialista destacó la utilidad estratégica de estas operaciones para combatir la delincuencia digital organizada, aunque también subraya la necesidad de actualizar la normativa, establecer mecanismos de control y

salvaguardar los derechos fundamentales, especialmente la intimidad de terceros no vinculados al caso.

Tabla 2

Análisis de la entrevista a un abogado penalista sobre agentes encubiertos informáticos

Preguntas	Respuesta del abogado especialista	Análisis
1. ¿Cuál es la importancia de las operaciones encubiertas en la investigación preprocesal?	Son fundamentales para la obtención de pruebas determinantes y la desarticulación de organizaciones criminales.	Son altamente útiles, siempre que se desarrollen conforme a normas claras para evitar vulneraciones de derechos fundamentales.
2. ¿Fue necesaria la implementación de los agentes encubiertos informáticos en el COIP?	Sí. La creciente incidencia de delitos informáticos en Ecuador y a nivel global hizo imprescindible su inclusión en la legislación penal.	La incorporación fue adecuada, aunque se requiere una actualización normativa constante para adaptarse a los avances tecnológicos.
3. ¿Cuáles son las características jurídicas de un agente encubierto informático?	Actúa previa autorización fiscal o judicial, bajo confidencialidad, sin incitar delitos, y se limita al entorno digital.	Es indispensable establecer mecanismos de control y capacitación que garanticen su actuación dentro del marco legal.
4. ¿Es correcto que esté libre de responsabilidad civil o penal?	Sí, siempre que su conducta se ajuste a la ley y respete el principio de proporcionalidad.	La exención debe estar sujeta a límites claros y a una supervisión efectiva para evitar abusos en el ejercicio de sus funciones.
5. ¿Puede afectar la intimidad de personas ajenas a la investigación?	Sí, existe el riesgo de acceder incidentalmente a información de terceros no vinculados al caso.	Es necesario implementar filtros técnicos y legales para garantizar la protección de los datos personales de terceros.

El abogado penalista entrevistado resaltó que las operaciones encubiertas desempeñan un papel clave en la etapa preprocesal, al permitir la obtención de pruebas fundamentales para la desarticulación de estructuras criminales complejas. Desde su perspectiva, estas operaciones resultan altamente efectivas siempre que se desarrollen dentro de un marco normativo claro, que garantice el respeto de los derechos fundamentales y evite excesos en su ejecución (Proaño, 2018).

Respecto a la inclusión del agente encubierto informático en el COIP, el especialista señaló que esta medida fue necesaria ante el creciente número de delitos informáticos tanto en Ecuador como a nivel internacional. Consideró que esta figura jurídica responde a la necesidad de que el sistema penal pueda enfrentar de forma eficaz la criminalidad digital. No obstante, advirtió que la normativa debe actualizarse de manera constante, para adaptarse a los avances tecnológicos y asegurar una aplicación adecuada.

En cuanto a sus características jurídicas, explicó que el agente encubierto informático actúa previa autorización del fiscal y, en ciertos casos, del juez competente. Su labor se rige por estrictos principios de confidencialidad, está prohibido que incite a cometer delitos y su campo de actuación se limita

exclusivamente al entorno digital. Para garantizar la legalidad de su intervención, el abogado recomendó establecer mecanismos de control y procesos de formación técnica que aseguren el cumplimiento estricto del marco legal.

Al referirse a la posibilidad de eximir al agente encubierto informático de responsabilidad civil o penal, el entrevistado afirmó que esta es válida únicamente si su conducta se ajusta plenamente a la ley y al principio de proporcionalidad. En caso contrario, debe ser sancionado como cualquier otro ciudadano. En este sentido, subrayó que la exención prevista en el COIP solo es aplicable cuando el agente actúa dentro de sus atribuciones legales, por lo que es fundamental contar con sistemas de supervisión que prevengan abusos (Contreras-Molina & Rodríguez-Hurtado, 2024).

Al finalizar, el abogado advirtió sobre el riesgo de que, durante el ejercicio de sus funciones, el agente acceda accidentalmente a información sensible de personas ajenas a la investigación penal. Aunque esto podría considerarse un daño colateral, no constituye una vulneración del derecho a la intimidad mientras dicha información no sea utilizada ni divulgada. Aun así, recomendó implementar filtros técnicos y legales que protejan los derechos de terceros no vinculados al caso investigado, reforzando así las garantías del debido proceso (Constitución de la República del Ecuador, 2008, art. 66).

La tabla 3 presenta las apreciaciones de un abogado especialista en criminalística respecto a las metodologías empleadas por los agentes encubiertos informáticos, así como las limitaciones necesarias para garantizar un accionar adecuado. A través de sus respuestas, se ofrece una perspectiva técnica y práctica sobre el funcionamiento de estos agentes en el entorno digital, resaltando los requisitos de formación, los riesgos inherentes a su labor y la necesidad de establecer límites que protejan los derechos fundamentales. El análisis subraya la importancia de contar con protocolos bien definidos, auditorías técnicas y un marco normativo específico que asegure una actuación proporcional, legal y ética en el ámbito del proceso penal.

El abogado especialista en criminalística señaló que la diferencia principal entre un agente encubierto tradicional y uno informático radica en el entorno en el que operan. Mientras el primero actúa en el mundo físico mediante infiltraciones directas en grupos delictivos, el segundo realiza sus funciones en entornos virtuales, accediendo a redes, foros o sistemas digitales. No obstante, ambos comparten el objetivo común de recolectar pruebas y desmantelar estructuras criminales organizadas. Por esta razón, es fundamental que cuenten con protocolos adaptados a sus respectivos contextos operativos, especialmente en el caso del agente informático, cuya actividad debe estar enmarcada en una regulación que contemple las particularidades del ciberespacio (Quezada-Quizhpe & Gende-Ruperti, 2025).

Tabla 3

Análisis de la entrevista a un abogado especialista en criminalística sobre metodología y limitaciones

Pregunta	Respuesta del especialista en criminalística	Análisis
1. ¿Cuál es la principal diferencia y semejanza entre un agente encubierto tradicional y un agente encubierto informático?	El tradicional actúa en el mundo físico; el informático en el entorno virtual. Ambos buscan obtener pruebas y desmantelar grupos delictivos.	Es clave que ambos tengan protocolos adecuados al entorno en el que operan. La regulación debe contemplar las particularidades del entorno digital.

2. ¿Cuál es la metodología utilizada por el agente encubierto informático en el ejercicio de sus funciones?	Usa programas instalados en su equipo para acceder a computadoras o celulares de los investigados. También apoya la ciberseguridad institucional.	Debe limitarse el uso de herramientas a fines legítimos y verificarse su uso a través de auditorías técnicas.
3. ¿Cómo se lleva a cabo la selección y entrenamiento de un agente encubierto informático para operar en el entorno digital?	Debe realizar cursos, pasar pruebas de actitud y aptitud, y tener conocimientos en software o ingeniería tecnológica.	Es fundamental certificar sus competencias éticas y técnicas mediante estándares oficiales y actualizados.
4. ¿Cuáles son los riesgos que pueden tener las operaciones de un agente encubierto informático en el ciberespacio?	Si son descubiertos, su vida puede estar en peligro. Además, pueden acceder a información privada de personas no relacionadas con la investigación.	Se deben establecer límites claros al acceso a datos, así como mecanismos de protección y denuncia en caso de vulneraciones.
5. ¿Qué limitaciones podrían establecerse para evitar que las operaciones de los agentes encubiertos informáticos violenten el derecho a la intimidad de terceras personas ajenas a la investigación penal?	Control estricto sobre qué información puede acceder, recolección solo de lo necesario, exámenes de capacidad y reglamentos específicos.	Es urgente contar con un marco normativo técnico-jurídico que regule sus actividades y evite abusos.

Respecto a la metodología utilizada, el especialista explicó que los agentes encubiertos informáticos emplean software especializados que les permiten ingresar, de forma oculta, a los dispositivos electrónicos de los investigados, como computadoras o teléfonos móviles. Asimismo, brindan apoyo en tareas de ciberseguridad institucional, fortaleciendo la protección de infraestructuras críticas. Sin embargo, enfatizó que el uso de estas herramientas debe limitarse estrictamente a fines legítimos y justificables, y estar sujeto a auditorías técnicas que controlen y verifiquen su correcta aplicación (Alanis et al., 2024).

En relación con su proceso de formación, indicó que los agentes encubiertos informáticos deben atravesar un proceso riguroso de selección, el cual incluye pruebas de actitud y aptitud, además de una preparación técnica específica en áreas como software, redes, ingeniería informática o seguridad digital. Esta capacitación debe estar respaldada por certificaciones actualizadas que incluyan estándares éticos y técnicos, ya que su actuación no solo implica conocimientos tecnológicos, sino un alto nivel de responsabilidad en el manejo de información sensible (Nieves-Lahaba & Ponjuán- Dante, 2021).

El especialista destacó que la labor del agente encubierto informático conlleva riesgos significativos, como posibles represalias si se revela su identidad y el acceso involuntario a datos personales de terceros ajenos a la investigación. Para mitigar estos riesgos, deben establecerse límites sobre la información accesible y garantizar mecanismos que protejan los derechos de terceros. Asimismo, subrayó la necesidad urgente de un marco normativo técnico-jurídico que regule sus funciones, defina criterios de idoneidad, y establezca directrices claras sobre el acceso, manejo de información digital y procedimientos operativos.

4. Discusión

Los hallazgos de esta investigación sobre la metodología utilizada por el agente encubierto informático en la recopilación de pruebas, y su impacto en el derecho a la intimidad de terceras personas no vinculadas con la investigación penal, permiten identificar riesgos significativos en el marco jurídico vigente. Al contrastar estos resultados con el aporte de juristas como López & García-Erazo (2023) y Enríquez (2021), se observa que las técnicas empleadas por estos agentes como infiltrarse en organizaciones delictivas o hackear redes, grupos o medios electrónicos pueden vulnerar el derecho constitucional a la intimidad. Esta afectación ocurre cuando, incluso de manera accidental, se accede a contenido multimedia perteneciente a personas que no forman parte de la investigación y sin su autorización previa. Ante este escenario, se hace evidente la necesidad de desarrollar un reglamento específico que regule con claridad las actuaciones de los agentes encubiertos informáticos, delimitando el acceso y tratamiento de información privada.

Las respuestas obtenidas en entrevistas a abogados en libre ejercicio revelan una dualidad en la percepción jurídica: mientras algunos consideran que las actuaciones de los agentes encubiertos informáticos se encuentran normadas y ajustadas al derecho vigente, otros plantean la urgencia de establecer restricciones adicionales. Un abogado especialista en derecho penal afirma que estas prácticas están contempladas en el ordenamiento jurídico y que cualquier extralimitación puede ser sancionada conforme a la ley. Por su parte, el abogado experto en criminalística sugiere adoptar mecanismos preventivos para evitar que los agentes accedan a información personal de terceros que no están involucrados en la investigación, con el fin de proteger derechos fundamentales.

En relación con la metodología específica empleada por los agentes encubiertos informáticos, se identificó el uso de programas automatizados para vulnerar contraseñas, así como la instalación de software en dispositivos electrónicos sin el consentimiento de sus propietarios. Estas prácticas, aunque efectivas para obtener evidencia en casos de delitos cibernéticos, no discriminan entre información relevante y aquella que pertenece a individuos ajenos a la causa penal. De esta forma, se corre el riesgo de incurrir en violaciones al derecho a la intimidad, garantizado por la Constitución. Por ello, se reitera la importancia de contar con un marco regulatorio que limite de manera precisa las actuaciones de estos agentes, garantizando el respeto a los derechos de personas no investigadas (Sarmiento-Chamba & Maldonado-Ruiz, 2024).

Para evitar abusos y garantizar el respeto a los derechos fundamentales, es imprescindible que las acciones de los agentes encubiertos informáticos cuenten con autorización judicial previa, justificada y limitada en alcance. Además, se deben implementar auditorías técnicas periódicas que supervisen sus actuaciones y aseguren transparencia. Estos mecanismos permitirían controlar el uso de herramientas intrusivas y proteger la intimidad de terceros ajenos a la investigación penal.

5. Conclusiones

La metodología utilizada por el agente encubierto informático, en la recopilación de pruebas en los delitos cibernéticos se encuentran reguladas por el COIP, sin embargo, este no prevé sobre la posibilidad de que ocurran descubrimientos adicionales y tampoco limita las funciones de estos agentes y hasta donde pueden llevar sus actividades en el marco de su trabajo.

Las actuaciones de los agentes encubiertos informáticos guardan estricta relación con el derecho a la intimidad. Cuando estos servidores policiales hackean una red o dispositivos electrónico de cualquier persona, automáticamente tiene acceso a su vida personal, por lo cual, es claro que sus

actividades se centran en invadir la privacidad de los investigados, la propia ley lo permite previa autorización debidamente fundamentada.

La falta de limitación en las actuaciones de los agentes encubiertos informáticos, y su afectación al derecho a la intimidad de las terceras personas ajenas al proceso penal, tiene como efecto violentar de manera directa norma expresa de alto rango como es la Constitución de la República del Ecuador, y que las personas que no son arraigadas a la investigación, sufran un ataque injustificado hacia su vida privada de manera indirecta, así no se hackee sus servidores, se está obteniendo información y contenido donde ellos están involucrados, lo que claramente nunca fue consentido por la potencial víctima.

Referencias

Alanis, E., López, E., Colín, J. M., Viñas, S., & Sosa, A. (2024). Ciberseguridad: impacto y detección de eventos de seguridad mediante prototipo de monitoreo. *Ciencia Latina Revista Científica Multidisciplinar*, *8*(3), 2975-2989. https://doi.org/10.37811/cl_rcm.v8i3.11511

Bravo, R. (2010). *La prueba en materia penal*. Universidad de Cuenca. https://n9.cl/742js

Cevallos, A. (28 de junio de 2023). Análisis jurídico del agente encubierto informático en el derecho penal ecuatoriano. *Lexis*. https://n9.cl/uawao

Código Orgánico Integral Penal [COIP]. Ley Orgánica, Art. 178, Art. 179, Art. 190, Art 483. 10 de febrero de 2014 (Ecuador).

Constitución de la República del Ecuador [CRE]. Art. 66, Art. 76. 20 de octubre de 2008 (Ecuador).

Contreras-Molina, A., & Rodríguez-Hurtado, B. (2024). Ciberacoso, una amenaza real para los jóvenes cubanos en la era digital. *Debate Jurídico Ecuador*, *7*(2), 148-157. https://doi.org/10.61154/dje.v7i2.3513

Enríquez, L. (15 de junio de 2021). *La ciberdelincuencia organizada I: diferencia entre hacktivistas y mercenarios*. Universidad Andina Simón Bolívar. https://n9.cl/pvrld

Fiscalía General del Estado & Policía Nacional del Ecuador. (2022). *Manual de procedimientos investigativos*. Sistema Especializado Integral de Investigación, Medicina Legal y Ciencias Forenses. https://n9.cl/oxozo

Juca-Maldonado, F., & Medina-Peña, R. (2023). Ciberdelitos en Ecuador y su impacto social; panorama actual y futuras perspectivas. *Portal de la Ciencia*, *4*(3), 325-337. https://doi.org/10.51247/pdlc.v4i3.394

López, P., & García-Erazo, E. (2023). La citación electrónica frente al principio de celeridad procesal. *Revista Científica Cultura, Comunicación y Desarrollo*, *8*(3), 242-249. https://rccd.ucf.edu.cu/index.php/aes/article/view/532

Montalbano, L. (2019). *El reglamento europeo de protección de datos personales y el derecho al olvido* [Tesis de doctorado, Universidad Complutense de Madrid]. Repositorio institucional. https://n9.cl/himnxg

Nieves-Lahaba, Y., & Ponjuán-Dante, G. (2021). Tratamiento de datos personales y acceso a la información: Visiones a partir de la academia. *Universitas - Revista de Ciencias Sociales y Humanas, 35*, 167–185. https://doi.org/10.17163/uni.n35.2021.08

Oficina de las Naciones Unidas contra la Droga y el Delito. (2013). *Manual de Técnicas Especiales de Investigación. Agente encubierto y entrega vigilada*. https://n9.cl/hwkms

Pazmiño, A. (2023). *Agente encubierto informático: su viabilidad en el proceso penal ecuatoriano* [Tesis de pregrado, Universidad Tecnológica ECOTEC]. Repositorio institucional. https://n9.cl/sec7l

Proaño, G. (2018). La necesidad de incorporar al agente encubierto cibernético en la Legislación Ecuatoriana. *Iuris Dictio*, (22), 217-228. https://doi.org/10.18272/iu.v22i22.1127

Quezada-Quizhpe, A., & Gende-Ruperti, C. (2025). Delito de ciber extorsión: un análisis jurídico, y comparativo en países de Latinoamérica, Perú, Colombia y Ecuador. *593 Digital Publisher CEIT*, *10*(1), 546-556. https://doi.org/10.33386/593dp.2025.1.2893

Sandoval, L. (2023). *Aplicabilidad de las operaciones encubiertas en el delito de delincuencia organizadaen el Ecuador* [Tesis de maestría, Universidad de las Américas]. Repositorio institucional. https://n9.cl/df93q0

Sarmiento-Chamba, J. A., & Maldonado-Ruiz, L. (2024). Delitos informáticos y ciberataques: análisis jurídico en el derecho penal del Ecuador. *MQRInvestigar*, *8*(3), 1753-1781. https://doi.org/10.56048/MQR20225.8.3.2024.1753-1781

Sotomayor, A. (11 de agosto 2024). El agente encubierto informático en el Ecuador. *La Barra Espaciadora*. https://n9.cl/xfipd

Villa, J., & Calle, N. C. (2023). Análisis del derecho a la intimidad personal y familiar en la difusión de videos e imágenes de ebrios consuetudinarios y toxicómanos en redes sociales. *Pacha*, *4*(12), e230209. https://doi.org/10.46652/pacha.v4i12.209

Yánez, P. (2017). *La figura del agente encubierto en el sistema penal ecuatoriano* [Tesis de pregrado, Universidad de Cuenca]. Repositorio institucional. https://n9.cl/w6f9q

Transparencia

Conflicto de interés

Los autores declaran que no existen conflictos de interés que influyan en la objetividad de este estudio.

Fuente de financiamiento

No se recibieron fondos financieros de ninguna organización que pudiera tener interés en los resultados presentados.

Contribución de autoría

Jhonatan Daniel Almeida Mancheno: Conceptualización, metodología, software, validación, análisis formal, investigación, visualización, redacción - preparación del borrador original, redacción - revisión y edición, financiamiento, administración del proyecto, recursos, supervisión.

Jorge Marcelo Quintana Yánez: Conceptualización, metodología, validación, análisis formal, investigación, visualización, redacción - preparación del borrador original, redacción - revisión y edición, financiamiento, recursos.

Los autores contribuyeron activamente en el análisis de los resultados, revisión y aprobación del manuscrito final.