Vol.8 No.3 (2024): Journal Scientific MQRInvestigar ISSN: 2588–0659
https://doi.org/10.56048/MQR20225.8.3.2024.4555-4574

The standard of proof in organized crime offenses

El estándar probatorio en delitos en la delincuencia organizada

Autores:

Arias-Becerra, Cristian Agustín
UNIVERSIDAD CATÓLICA DE CUENCA
Cuenca – Ecuador
cristian.arias@est.ucacue.edu.ec
https://orcid.org/0009-0005-8043-1664

Monsalve-Robalino, Bernardo Xavier
UNIVERSIDAD CATÓLICA DE CUENCA
Cuenca – Ecuador
bernardo.monsalve@ucacue.edu.ec
https://orcid.org/0009-0009-5509-8184

Fechas de recepción: 01-AGO-2024 aceptación: 02-SEP-2024 publicación: 15-SEP-2024

https://orcid.org/0000-0002-8695-5005

http://mqrinvestigar.com/

Resumen

Este estudio se enfoca en la problemática de la evidencia digital en casos de delincuencia organizada, considerando la creciente influencia de la tecnología en la comisión de estos delitos y su impacto en los estándares probatorios. Dada la sofisticación tecnológica de las organizaciones criminales, la recolección y presentación de pruebas digitales en los tribunales plantea desafíos significativos para el sistema de justicia penal. El objetivo principal es analizar cómo la evolución de la tecnología ha influido en la naturaleza y la complejidad de la evidencia digital en casos de delincuencia organizada, así como examinar las implicaciones de estos cambios en los estándares probatorios y la administración de justicia. Para abordar este objetivo, se utilizó una metodología que incluyó revisión bibliográfica con enfoque cualitativo en la cual, se revisa la información disponible en los principales repositorios digitales. Los resultados principales revelaron una serie de desafíos en la recolección, preservación y presentación de evidencia digital en casos de delincuencia organizada, incluyendo la dificultad para establecer la autenticidad y la integridad de la evidencia, así como la falta de estándares claros en el manejo de pruebas digitales en el sistema legal. Estos hallazgos subrayan la necesidad de revisar y adaptar los estándares probatorios para abordar los desafíos tecnológicos emergentes y garantizar una administración de justicia efectiva y equitativa en un entorno digitalizado. En conclusión, el estudio destaca la importancia de una actualización constante del marco legal para hacer frente a la evolución de la tecnología y sus implicaciones en la lucha contra la delincuencia organizada.

Palabras clave: Estándar probatorio, delincuencia organizada, tecnología

Abstract

This study focuses on the issue of digital evidence in organized crime cases, considering the growing influence of technology in the commission of these crimes and its impact on evidentiary standards. Given the technological sophistication of criminal organizations, the collection and presentation of digital evidence in court poses significant challenges for the criminal justice system. The main objective is to analyze how the evolution of technology has influenced the nature and complexity of digital evidence in organized crime cases, as well as to examine the implications of these changes on evidentiary standards and the administration of justice. To address this objective, we used a methodology that included a qualitative literature review in which we reviewed the information available in the main digital repositories. Key findings revealed a number of challenges in the collection, preservation and presentation of digital evidence in organized crime cases, including the difficulty in establishing the authenticity and integrity of evidence, as well as the lack of clear standards in the handling of digital evidence in the legal system. These findings underscore the need to review and adapt evidentiary standards to address emerging technological challenges and ensure effective and fair administration of justice in a digitized environment. In conclusion, the study highlights the importance of constantly updating the legal framework to cope with the evolution of technology and its implications in the fight against organized crime.

Keywords: Evidentiary standard, organized crime, technology

Introducción

La Delincuencia Organizada (DO) ha experimentado un rápido desarrollo y se ha situado a la vanguardia de las Tecnologías de la Información y la Comunicación (TIC). Desde 2017, la International Police (INTERPOL) ha informado que el crimen organizado a nivel mundial ha aprovechado las facilidades del comercio, el acceso inmediato a la información y el uso de comunicaciones cifradas, creando un ambiente propicio para el florecimiento de la actividad delictiva. Los grupos delictivos pueden adaptar rápidamente sus operaciones y modelos de actividad para aprovechar las oportunidades y demandas cambiantes del entorno (Secretaría General de INTERPOL, 2017).

Por otro lado, la Global Initiative Against Transnational Organized Crime (2023), en su informe, resalta el uso extendido de plataformas de comunicación encriptada, como EncroChat y Sky ECC, entre estos grupos criminales, lo que garantiza un alto grado de anonimato y seguridad en sus comunicaciones, dificultando así su rastreo. Esta adaptabilidad presenta un desafío adicional para las autoridades encargadas de hacer cumplir la ley y procesar a estos ciminales, quienes deben mantenerse al día con las estrategias en constante evolución de los delincuentes.

Las estrategias avanzadas empleadas por la DO mediante el uso de tecnología representan un desafío significativo en el proceso de enjuiciamiento de estos grupos criminales, particularmente en lo que respecta a la presentación de pruebas. La información crucial que podría servir para incriminar de manera inequívoca las actividades delictivas de estas organizaciones suele estar encriptada, suplantada o resulta difícil de atribuir al imputado debido al uso de redes privadas (Saca et al., 2024). Como consecuencia, el debido proceso en estos casos se ve considerablemente obstaculizado, lo que conlleva a un aumento en la impunidad de los grupos delictivos que emplean la tecnología para encubrir sus acciones ante las autoridades.

Kovacs et al. (2023) resaltan los desafíos asociados con la presentación de pruebas en casos de delincuencia organizada, especialmente debido a la naturaleza digital de la evidencia. Estos desafíos incluyen la complejidad técnica y especializada de la evidencia digital, que puede requerir la asistencia de expertos para su comprensión adecuada. Además, existe el riesgo de malinterpretaciones por parte de los abogados, lo que podría ser aprovechado por la defensa criminal. La gran cantidad de datos a analizar y los plazos ajustados también

representan dificultades adicionales para la fiscalía, dificultando un análisis exhaustivo de la información presentada.

Desde una perspectiva local, la Policía Nacional del Ecuador, a través de la DINASED y el Departamento de Seguridad de las TIC (DNTIC), ha presentado informes en 2021 y 2023 respectivamente que destacan un aumento en el uso de estrategias tecnológicas por parte de la DO en el país y que pueden dificultar la presentación de medios probatorios. Estas estrategias incluyen la encriptación de datos para dificultar el rastreo de sus actividades, el robo de identidad para cometer ilícitos, y el uso de Redes Privadas Virtuales (VPN) para ocultar movimientos y complicar la identificación de la ubicación desde donde se cometen estos actos, entre otras tácticas identificadas (DNTIC, 2023; DINASED, 2021).

Ante la problemática anterior mencionada, la presente investigación se plantea la siguiente pregunta: ¿De qué manera la sofisticación operativa de la delincuencia organizada en Ecuador influye en la efectividad de los estándares probatorios durante la persecución judicial de estos crímenes? Para responder a esta pregunta, se esboza el siguiente objetivo general: Evaluar cómo las tácticas evasivas y el uso de tecnologías de seguridad digital por parte de la delincuencia organizada en Ecuador afectan la capacidad de los fiscales para cumplir con los estándares probatorios requeridos en la persecución legal de estos delitos.

Para cumplir con el objetivo anterior planteado, se propone identificar las principales tácticas evasivas y tecnologías de seguridad digital utilizadas por la delincuencia organizada en Ecuador. Ahondando a esto también se analiza el impacto de estas tácticas y tecnologías en la eficacia de la recopilación de pruebas por parte de los fiscales y se realiza una evaluación de las brechas y desafíos en los estándares probatorios actuales frente a las estrategias avanzadas de la delincuencia organizada.

La relevancia de este estudio reside en la necesidad imperativa de realizar una evaluación exhaustiva sobre cómo las tácticas evasivas y el empleo de tecnologías de seguridad digital por parte de la delincuencia organizada (DO) en Ecuador afectan la capacidad de los fiscales para recopilar pruebas y cumplir con los estándares probatorios exigidos en la persecución legal de estos delitos. Este análisis permitirá poner de manifiesto y comprender las estrategias utilizadas por estos grupos delictivos en el país, lo que a su vez facilitará una acción efectiva por parte de las autoridades para combatir este tipo de criminalidad.

La metodología empleada en esta investigación consistió en una revisión bibliográfica, no experimental, descriptiva, con un enfoque cualitativo. Se recopiló información relevante de diversas fuentes en línea sobre las principales categorías evaluadas, contrastándolas entre sí para alcanzar conclusiones alineadas con los objetivos del estudio.

Metodología

La investigación presentada fue una revisión bibliográfica de tipo no experimental, descriptiva y con un enfoque cualitativo, lo que implica que no se manipularon variables y se basó únicamente en el análisis y descripción de información proveniente del entorno académico. Este estudio se enfocó en explorar, a través de los aportes de diversos autores, el estándar probatorio en casos de delincuencia organizada para identificar los desafíos que enfrenta el sistema judicial ecuatoriano al enjuiciar a los miembros de estas organizaciones criminales.

El proceso de recolección de información inició con la selección de repositorios científicos en la red, específicamente aquellos con convenios con la Universidad Católica de Cuenca, como Scopus, Research Gate, Scielo y Dialnet, entre otros. Además, se utilizó información proveniente de fuentes verificadas encontradas en Google Académico. Una vez identificados los repositorios, se procedió a aplicar operadores booleanos como “AND”, “OR”, y “Y” para realizar combinaciones de palabras que permitieran efectivizar la búsqueda en la red, tales como: “estándar probatorio” and “delincuencia organizada” or “delincuente” and “jurisprudencia”, entre otras combinaciones. Después de aplicar las palabras clave, se obtuvo una base de datos completa que abordaba la temática analizada en esta investigación, la cual fue dispuesta en fichas bibliográficas. Para el cribado de la información y la selección de artículos relevantes, se aplicaron los siguientes criterios de elegibilidad:

Criterios de elegibilidad

- Investigaciones actualizadas, de los últimos 5 años
- Artículos publicados que aborden dentro de su título, resumen o contenidos las categorías de análisis de esta investigación
- Documentos en idioma español o inglés

Criterios de rechazo

- Investigaciones sin sustento comprobable de sus afirmaciones

- Documentos que no incluyan dentro de su título o resumen algunas de las palabras clave analizadas
- Literatura gris, tesis de pregrado, monografías y otros tipos de documentos que no recae dentro del rigor académico de esta investigación.

Estos criterios sirvieron para realizar un primer cribado de la información. Sin embargo, fue necesario realizar una lectura crítica de los documentos para seleccionar y clasificar los artículos que cumplían con los objetivos esbozados en la presente investigación.

Resultados

En este apartado se presentan los resultados más relevantes sobre las tácticas evasivas de la delincuencia organizada en el uso de la tecnología y medios digitales. Se analiza el estándar probatorio en estos casos y el marco normativo sobre la presentación de pruebas en esta situación. Además, en cada uno de los apartados mencionados, se incluye un análisis y discusión entre autores para contrastar las teorías y afirmaciones de los documentos revisados.

Tácticas evasivas y uso de tecnologías de la delincuencia organizada

La DO se caracteriza típicamente por la presencia de un grupo bien estructurado de individuos que operan bajo un liderazgo claro y participan en actividades ilegales para obtener ganancias financieras. Estas estructuras criminales presentan similitudes con una institución estructurada, con elementos como: una clara distribución de responsabilidades, acciones coordinadas guiadas por reglas y códigos, y la delegación de tareas específicas para lograr objetivos específicos (Zabyelina, 2023).

El nivel de tecnificación y organización alcanzado por estas estructuras criminales ha llevado sus actividades a un grado de sofisticación que actualmente representa un desafío tanto técnico como legal para su procesamiento. Estos desafíos abarcan un amplio espectro de actividades delictivas, como delitos económicos, delitos cibernéticos, actividades ilícitas en la web oscura, actos de terrorismo y explotación sexual en línea. Es crucial señalar que los requisitos de evidencia y las técnicas para reunir dicha evidencia se han vuelto cada vez más complejos para navegar por el sistema de justicia penal (Deslauriers-Varin y Fortin, 2021).

Una estrategia común utilizada por estos grupos para evadir la justicia con ayuda de la tecnología implica el manejo de fondos generados por actividades criminales. Según la investigación de Di-Nicola (2022), la utilización de monedas tecnológicas como las criptomonedas ofrece varias ventajas al crimen organizado. Estas incluyen la capacidad de realizar transacciones financieras con anonimato y privacidad, acelerar las transferencias globales de fondos sin intermediarios, eludir las regulaciones financieras tradicionales y facilitar el lavado de dinero a través de transacciones que son difíciles de rastrear en la red blockchain.

Según Leuprecht et al. (2022) el lavado de dinero mediante el uso de monedas digitales, como las criptomonedas, implica la conversión de fondos ilícitos en apariencia de activos legítimos mediante transacciones en línea que se benefician del anonimato y la descentralización inherentes a estas monedas. Este proceso complica la capacidad de rastrear los flujos financieros e identificar a los responsables del delito, lo que representa un desafío significativo para las políticas actuales de prevención del lavado de dinero. La naturaleza transfronteriza y virtual de las criptomonedas dificulta la supervisión y regulación por parte de las autoridades, lo que puede facilitar la ocultación de actividades delictivas y el lavado de dinero a gran escala, enfatizando la necesidad de adaptar las políticas existentes para abordar esta nueva forma de delincuencia financiera.

Otra táctica evasiva empleada por ciertas estructuras criminales en el ciberespacio implica el uso de encriptación digital para respaldar operaciones delictivas y facilitar la comunicación interna. La encriptación digital sirve como una herramienta que protege las comunicaciones y los datos sensibles de los ciberdelincuentes, impidiendo que sean interceptados o descifrados por terceros no autorizados. Esto permite que las estructuras criminales se organicen, deleguen responsabilidades, planifiquen actividades ilícitas e incluso desarticulen operaciones antes de que las autoridades ejecuten acciones, sin dejar evidencia punible que pueda ser utilizada en su contra ante un tribunal (Jakubiec, 2022).

La encriptación en dispositivos móviles usados por delincuentes representa un desafío para la informática forense al codificar datos y dificultar accesos no autorizados. Anteriormente, los datos almacenados permitían una recuperación más sencilla, pero con la implementación de medidas de seguridad avanzadas, la encriptación obstaculiza la extracción convencional de datos. Además, técnicas destructivas como el "chip-off" pueden dañar componentes

vitales para descifrar los datos. La encriptación también complica la recuperación de datos eliminados, ya que las funciones de eliminación segura pueden borrarlos de manera efectiva dificultando de manera exhaustiva la incautación de medos probatorios (Fukami et al., 2021). Según Koops y Leenes (2020) el robo de identidad representa otra táctica empleada por la delincuencia organizada para perpetrar una amplia gama de actividades delictivas, que incluyen desde: el fraude con tarjetas de crédito hasta el lavado de dinero, el tráfico de drogas, el terrorismo y otros crímenes. La habilidad de los delincuentes para utilizar identidades falsas o robadas les permite ocultar sus acciones ilícitas y dificulta su detección y aprehensión por parte de las autoridades.

De acuerdo con Ilzan et al. (2023), la identificación de individuos implicados en casos de robo de identidad puede presentar dificultades significativas por diversas razones. En primer lugar, al usurpar la identidad de terceros, los perpetradores pueden ocultar su verdadera identidad, camuflando así transacciones fraudulentas bajo una apariencia legítima. Además, suelen recurrir a técnicas sofisticadas, como el uso de redes informáticas anónimas o la manipulación de datos digitales, para obstaculizar su rastreo por parte de las autoridades. La naturaleza global y digital de muchos de estos delitos también agrega complejidad a su identificación, dado que pueden operar más allá de fronteras internacionales y emplear métodos avanzados de ocultamiento.

La presencia de estructuras criminales organizadas, que operan bajo una clara jerarquía y coordinación, plantea desafíos técnicos y legales significativos en la lucha contra la delincuencia organizada. Estas organizaciones, cuyas actividades abarcan desde delitos económicos hasta el lavado de dinero y el terrorismo, han alcanzado niveles de sofisticación que desafían los métodos convencionales de persecución. Por ejemplo, el uso de criptomonedas facilita el lavado de dinero a través de transacciones difíciles de rastrear, mientras que la encriptación digital protege las comunicaciones y datos de los ciberdelincuentes. Además, el robo de identidad dificulta la detección de los responsables, ya que pueden ocultar sus actividades ilegales bajo identidades falsas o robadas, aprovechando la complejidad del entorno digital y globalizado en el que operan.

La complejidad técnica y la naturaleza transfronteriza de la delincuencia organizada plantean un desafío adicional para las autoridades encargadas de hacer cumplir la ley. La dificultad para rastrear los flujos financieros, identificar a los responsables y reunir pruebas suficientes

para su procesamiento ante la justicia subraya la necesidad de adaptar las políticas y técnicas de investigación existentes. Las medidas de seguridad avanzadas, como la encriptación en dispositivos móviles y el uso de identidades falsas, presentan obstáculos significativos para la informática forense y la identificación de los perpetradores.

En última instancia, hemos examinado a fondo diferentes facetas relativas a las esquivas estrategias empleadas por las OD, particularmente en el ámbito de la tecnología. Con la llegada de las tecnologías de seguridad digital, las criptomonedas y el cifrado de datos, las autoridades encargadas de hacer cumplir la ley han enfrentado desafíos sin precedentes en sus esfuerzos por investigar y procesar actividades delictivas. Además, la complejidad de estas estrategias ha llevado al desarrollo de un entorno en el que la detección y persecución legal de los criminales se vuelve cada vez más compleja. Dadas las circunstancias, es imperativo que los sistemas legales y los organismos encargados de hacer cumplir la ley mejoren y amplíen sus capacidades técnicas para combatir eficazmente la creciente actividad delictiva en el ámbito digital.

Estándar probatorio en casos de delincuencia organizada

La prueba desempeña un papel fundamental en la administración de justicia, ya que facilita la clarificación de los hechos en disputa y proporciona al juzgador una visión completa del caso en cuestión (Wang, 2020). Desde la perspectiva de los procedimientos legales, un estándar probatorio se emplea para determinar el grado de convicción necesario para establecer la veracidad de un hecho. Esta norma establece los criterios para la cantidad y calidad de las pruebas requeridas para respaldar la veracidad de una afirmación o acusación en un proceso judicial (Parra, 2022).

La presentación de pruebas y los estándares probatorios se encuentran ante diversos desafíos al momento de ser aceptados y validados en un proceso judicial contra miembros de la delincuencia organizada. En este sentido, es crucial abordar las dificultades que surgen, especialmente en relación con las tácticas evasivas empleadas por estos grupos criminales. A continuación, se enumeran algunos de estos obstáculos, destacando su relevancia en el contexto jurídico actual.

El uso de monedas digitales, como las criptomonedas, plantea un desafío significativo en la incautación y presentación de pruebas en casos de lavado de dinero. La naturaleza descentralizada y pseudoanónima de estas transacciones dificulta el seguimiento y la

vinculación efectiva de las mismas a individuos o entidades específicas. Además, ciertas criptomonedas están diseñadas específicamente para ocultar la identidad de los participantes y las transacciones, lo que complica aún más la capacidad de las autoridades para seguir el rastro del dinero en casos de lavado de dinero. Esta falta de transparencia y trazabilidad en las transacciones con criptomonedas dificulta la recopilación de pruebas sólidas para investigaciones y procesos legales relacionados con el lavado de dinero (Albrecht et al., 2019).

Según Gutiérrez (2019), el estándar probatorio en casos de delincuencia organizada, especialmente en lavado de activos, desempeña un papel crucial en su investigación y persecución. Dada la escasez de pruebas directas en este contexto, las pruebas indiciarias son fundamentales. Estas pruebas permiten inferir la existencia de un delito a partir de circunstancias o indicios, siendo especialmente relevantes en el lavado de activos, donde la ocultación del origen ilícito de los fondos es común. Es esencial que el uso de pruebas indiciarias respete los principios del debido proceso y la presunción de inocencia. Para ello, se requiere capacitación y especialización de las autoridades judiciales, así como recursos humanos y tecnológicos adecuados para una investigación justa y efectiva, sin vulnerar los derechos de los implicados.

En relación al estándar probatorio en los delitos informáticos, Arévalo (2019) señala que se debe destacar el papel fundamental que desempeña la evidencia digital en los procedimientos judiciales, pues puede resultar determinante para establecer la culpabilidad o inocencia en un caso. Al ser almacenada o transmitida en formato digital, esta evidencia proporciona detalles precisos sobre el delito o incidente en cuestión. Sin embargo, para ser considerada válida en los tribunales, debe cumplir con principios esenciales como autenticidad, integridad y confiabilidad. No obstante, es importante destacar que, debido a las estrategias de evasión, ocultamiento y tecnificación empleadas por la delincuencia en este ámbito, el proceso de recopilación y análisis de la evidencia digital se ha vuelto cada vez más complejo.

Paucar et al. (2021) señalan que las pruebas digitales en el contexto de los procesos judiciales en Ecuador, especialmente en relación con el Código Orgánico General de Procesos (COGEP) deben cumplir con ciertos requisitos para que estas pruebas sean válidas en el proceso judicial, como: la veracidad de la información, la firma electrónica, la obtención lícita de datos y la no alteración de los mismos. No obstante, estos mismos requisitos pueden

complicar su uso como medio probatorio, ya que la obtención lícita de datos puede ser difícil si la información está protegida o se necesita la colaboración de terceros, y garantizar la integridad de los datos puede ser desafiante en entornos digitales propensos a la manipulación. Aunque cruciales para la validez y confiabilidad de las pruebas digitales, su cumplimiento puede plantear desafíos en la práctica judicial.

Según Stoykova (2021) la relación entre la evidencia digital y el principio de presunción de inocencia en investigaciones criminales es de suma importancia para garantizar la equidad y la justicia en los procesos judiciales relacionados con la delincuencia organizada. La naturaleza de la evidencia digital plantea desafíos significativos en términos de fiabilidad y autenticidad, lo que podría comprometer la integridad del principio de presunción de inocencia si no se maneja adecuadamente. Es esencial abordar estas preocupaciones mediante la implementación de estándares rigurosos y procedimientos claros para validar la evidencia digital, protegiendo así los derechos de los sospechosos y asegurando un juicio imparcial y justo para todas las partes involucradas en casos de crimen organizado.

En el complejo entorno del crimen organizado y la ciberdelincuencia, los desafíos para la informática forense son innegables. La rápida evolución tecnológica y la diversidad de plataformas representan obstáculos considerables para la recolección y análisis de evidencia digital. Además, la falta de estándares claros y la necesidad de garantizar la integridad de dicha evidencia en los tribunales son preocupaciones fundamentales. Es esencial establecer regulaciones sólidas y fomentar la colaboración entre los sectores legal y tecnológico para abordar estos desafíos y garantizar una respuesta efectiva ante la ciberdelincuencia (Rakha, 2024).

En base al contenido presentado en este apartado, se puede discutir la información desde diferentes puntos de vista. En primer lugar, se destaca la dificultad que representan las criptomonedas en la investigación de lavado de dinero debido a su naturaleza pseudoanónima y descentralizada. La capacidad de rastrear y vincular transacciones a individuos específicos se ve obstaculizada, lo que afecta la capacidad de los fiscales para cumplir con los estándares probatorios exigidos por la ley. Esta dificultad refuerza la importancia de desarrollar métodos innovadores para la recolección de pruebas en casos de delincuencia organizada.

Por otro lado, se subraya la importancia de las pruebas indiciarias en casos de delincuencia organizada, especialmente en el contexto del lavado de activos. Estas pruebas, basadas en

circunstancias o indicios, son fundamentales cuando la evidencia directa es escasa. Sin embargo, es crucial garantizar que su uso respete los principios del debido proceso y la presunción de inocencia, lo que subraya la necesidad de capacitación y recursos adecuados para las autoridades judiciales.

Varios autores, como Arévalo (2019), Paucar et al. (2021) y Stoykova (2021), señalan los desafíos asociados con la evidencia digital en casos de crimen organizado. La integridad, autenticidad y confiabilidad de esta evidencia son cruciales para su admisibilidad en el tribunal. Sin embargo, la rápida evolución tecnológica y la complejidad de la ciberdelincuencia plantean obstáculos significativos en su recolección y análisis. Además, la necesidad de cumplir con requisitos específicos, como la obtención lícita de datos y la garantía de integridad, puede complicar su uso como medio probatorio.

Asimismo, es de suma importancia establecer regulaciones sólidas y fomentar la colaboración entre los sectores legal y tecnológico para abordar los desafíos asociados con la evidencia digital y la ciberdelincuencia. Esta colaboración es esencial para garantizar una respuesta efectiva ante la creciente sofisticación de los grupos criminales y la rápida evolución de la tecnología.

Marco normativo sobre estándar probatorio en la delincuencia organizada

En el sistema jurídico ecuatoriano, el estándar probatorio para la presentación de pruebas está regido por la Constitución y sus organismos derivados encargados de hacer cumplir la ley.

En específico, los artículos 76, numeral 4 y 82 de la Constitución son fundamentales en este contexto. El artículo 76.4 establece que las pruebas obtenidas o actuadas en violación de la Constitución o la ley carecen de validez probatoria, resaltando la importancia de la legalidad en la obtención de evidencia. Por su parte, el artículo 82 garantiza el derecho a la seguridad jurídica, que se basa en el respeto a la Constitución y en la existencia de normas jurídicas previas, claras y aplicadas por las autoridades competentes. En conjunto, estos artículos aseguran un proceso justo y equitativo, donde las pruebas presentadas sean obtenidas de manera legal y se respeten los derechos constitucionales de todas las partes involucradas.

En relación con el Código Orgánico Integral Penal (COIP) y su disposición sobre medios probatorios de tipo digital, se hace referencia a varios artículos que regulan diferentes aspectos relacionados con la recolección y presentación de pruebas digitales en un proceso judicial.

El artículo 477 establece el procedimiento para el reconocimiento de medios digitales, autorizando al fiscal a realizar este reconocimiento con la intervención de dos peritos que deben jurar guardar reserva. Además, el artículo 456 establece la cadena de custodia de elementos digitales utilizados como prueba, asegurando la integridad y autenticidad de las evidencias durante toda la investigación o proceso legal. Por otro lado, el artículo 460 aborda el reconocimiento del lugar de los hechos en el ámbito digital, aunque se señala una limitación en cuanto a la inclusión de pruebas digitales más sofisticadas, como las relacionadas con criptomonedas o sistemas de seguridad avanzados, que no son abordadas de manera específica en el reglamento establecido en el artículo 500.

Dentro del contexto de presentación de pruebas y el combate al crimen organizado, el Código Orgánico General de Procesos (COGEP) juega un papel crucial al regular el procedimiento en los procesos judiciales en Ecuador. Si bien el artículo 202 de este cuerpo legal establece que los documentos producidos electrónicamente, junto con sus anexos, son considerados originales para todos los efectos legales, esta disposición se limita a documentos escaneados y no aborda específicamente la presentación de pruebas digitales que no sean una copia de un documento físico. Por ende, la ausencia de un apartado relacionado con la presentación de pruebas digitales originales podría representar un desafío en la aplicación de pruebas indiciarias en casos de delincuencia organizada a través de medios digitales, especialmente cuando estas pruebas no pueden ser interpretadas íntegramente por un perito.

La discusión sobre si las leyes del país representan una traba al momento de presentar pruebas digitales implica considerar varios aspectos de la legislación ecuatoriana, incluyendo la Constitución, el Código Orgánico Integral Penal (COIP) y el Código Orgánico General de Procesos (COGEP).

En primer lugar, la Constitución de Ecuador establece principios fundamentales relacionados con el debido proceso y el respeto a los derechos constitucionales de las personas. Los artículos 76 y 82 de la Constitución garantizan que las pruebas presentadas en un proceso legal deben ser obtenidas de manera legal y respetando los derechos de las partes involucradas, así como la seguridad jurídica. Sin embargo, no proporciona una orientación específica sobre la presentación de pruebas digitales más avanzadas, como las relacionadas con criptomonedas o la seguridad informática.

Por otro lado, el COIP y el COGEP establecen procedimientos específicos para la presentación de pruebas en procesos judiciales. El COIP, en su artículo 477, regula el reconocimiento de medios digitales en un proceso judicial, mientras que el COGEP, en su artículo 202, reconoce la validez legal de documentos producidos electrónicamente, pero se limita a documentos escaneados y no aborda específicamente las pruebas digitales originales. Esta situación puede representar una traba en la presentación de pruebas digitales, especialmente en casos de delincuencia organizada donde el uso de tecnologías avanzadas y criptomonedas es común. La falta de disposiciones claras y específicas en la legislación ecuatoriana podría dificultar la admisibilidad de ciertas pruebas digitales en los tribunales, lo que podría limitar la capacidad de los fiscales para llevar a cabo investigaciones eficaces y obtener condenas en casos de crimen organizado.

Es decir, si bien las leyes del país establecen ciertas disposiciones relacionadas con la presentación de pruebas digitales, existe una falta de orientación específica sobre aspectos más avanzados de la tecnología digital, lo que podría representar una traba en la aplicación efectiva de la ley en casos de delincuencia organizada.

Discusión

El uso de la tecnología ha revolucionado el mundo de la delincuencia organizada de varias maneras significativas. Primero, la tecnología ha permitido que estas organizaciones operen a una escala global de manera más eficiente y discreta y esto tiene una implicación significativa en la sociedad. Por un lado, la sofisticación tecnológica de la delincuencia organizada puede llevar a un aumento en la comisión de delitos, así como a una mayor dificultad para detectar y procesar a los culpables.

Esto puede socavar la confianza en las instituciones encargadas de hacer cumplir la ley y generar un sentido de inseguridad en la población. Además, el aumento de la delincuencia organizada facilitado por la tecnología puede tener repercusiones económicas y sociales negativas, como el aumento del lavado de dinero, el fraude financiero y otros delitos financieros que afectan a empresas y ciudadanos comunes.

Los hallazgos sobre el estándar probatorio sobre los nuevos modos de operación de la delincuencia organizada revelan un panorama complejo en la administración de justicia,

donde la sofisticación tecnológica presenta desafíos significativos en la recolección y presentación de pruebas. La evasión a través de criptomonedas y la encriptación digital complica la trazabilidad de fondos y la autenticidad de la evidencia, mientras que la escasez de pruebas directas resalta la importancia de las pruebas indiciarias, requiriendo capacitación especializada y recursos adecuados para su utilización justa.

Además, se evidencia la necesidad de revisar y adaptar los estándares probatorios para abordar la complejidad de los delitos contemporáneos y garantizar una respuesta efectiva y equitativa en la persecución de la delincuencia organizada. La colaboración intersectorial entre el ámbito legal y tecnológico emerge como una pieza clave para enfrentar estos desafíos, promoviendo la adecuada aplicación de la ley sin comprometer los derechos fundamentales de los acusados.

Las implicaciones para la justicia ecuatoriana son significativas y multifacéticas. En primer lugar, la falta de disposiciones específicas para abordar los desafíos tecnológicos de la delincuencia organizada podría afectar la efectividad de los procesos judiciales. Esto podría resultar en dificultades para admitir y presentar pruebas digitales en casos donde la evidencia electrónica es fundamental.

Además, la ausencia de orientación clara en la legislación podría generar incertidumbre jurídica y desafíos en la interpretación y aplicación de la ley por parte de los tribunales. Esto podría conducir a decisiones judiciales inconsistentes y a una falta de coherencia en la jurisprudencia relacionada con la delincuencia organizada y las pruebas digitales.

Por otro lado, la adaptación del marco normativo a los nuevos desafíos tecnológicos requerirá esfuerzos legislativos significativos y una colaboración estrecha entre el poder judicial, los legisladores y otros actores relevantes. Esto podría implicar la revisión y modificación de leyes existentes, así como la implementación de nuevas disposiciones que aborden específicamente el uso de tecnología en la comisión de delitos y la presentación de pruebas en procesos judiciales.

En última instancia, estas implicaciones resaltan la necesidad de una actualización constante del marco legal para mantenerse al día con los avances tecnológicos y garantizar una administración de justicia eficaz y equitativa en un entorno cada vez más digitalizado.

Una limitación importante de este estudio radica en el enfoque centrado principalmente en la revisión bibliográfica y la recopilación de datos secundarios. Aunque esto proporciona una

visión amplia y fundamentada de los desafíos que enfrenta la justicia penal en casos de delincuencia organizada relacionados con el uso de tecnología, la falta de datos primarios podría limitar la comprensión completa de la situación en el terreno y la identificación de nuevas tendencias o perspectivas. Además, la naturaleza cambiante y dinámica de la tecnología y la delincuencia organizada podría implicar que algunas de las conclusiones alcanzadas en este estudio puedan volverse obsoletas con el tiempo.

Para investigaciones futuras, se sugiere realizar estudios empíricos que examinen de manera detallada el impacto de las tecnologías emergentes, como la inteligencia artificial y el blockchain, en la evolución de la delincuencia organizada y su influencia en los estándares probatorios. Además, sería beneficioso llevar a cabo investigaciones longitudinales que sigan de cerca la implementación y efectividad de nuevas políticas y regulaciones dirigidas a abordar los desafíos de la evidencia digital en casos de delincuencia organizada, con el fin de evaluar su impacto a lo largo del tiempo y identificar posibles áreas de mejora.

Conclusiones

Tras un análisis de la evidencia presentada en esta investigación, se concluye que la delincuencia organizada en Ecuador ha adoptado tácticas evasivas sofisticadas y tecnologías de seguridad digital avanzadas, lo que plantea serios desafíos para la recopilación y presentación de pruebas en el sistema judicial. Las organizaciones criminales utilizan criptomonedas y técnicas de encriptación digital para ocultar sus actividades, dificultando así la labor de las autoridades. Esta situación exige una actualización urgente de los marcos normativos y el fortalecimiento de las capacidades institucionales para enfrentar la complejidad y sofisticación de estos delitos. Es imperativo que se promueva una colaboración estrecha entre el sector legal y tecnológico, y se implemente una formación continua para los fiscales y agentes del orden, con el fin de garantizar una respuesta eficaz y equitativa ante la creciente amenaza de la delincuencia organizada en el entorno digital.

El análisis ha identificado y documentado las tácticas evasivas más comunes utilizadas por la delincuencia organizada en Ecuador. Esta identificación proporciona una visión clara de las estrategias empleadas por estos grupos para eludir la justicia y dificultar la recopilación de pruebas, lo que es crucial para diseñar contramedidas efectivas. El análisis del uso de

tecnologías de seguridad digital por la delincuencia organizada en Ecuador revela un alto nivel de sofisticación y adaptación a entornos tecnológicos complejos. Esta realidad plantea desafíos significativos para las autoridades encargadas de combatir el crimen organizado, subrayando la necesidad de actualización constante y formación en nuevas tecnologías para los organismos de seguridad.

La evaluación destaca cómo las tácticas evasivas y el uso de tecnologías de seguridad digital impactan negativamente en la eficacia de la recopilación de pruebas por parte de los fiscales. Esto evidencia la necesidad urgente de desarrollar estrategias y recursos especializados que contrarresten estas prácticas y aseguren la integridad del proceso judicial. La evaluación de las brechas y desafíos en los estándares probatorios actuales frente a las estrategias avanzadas de la delincuencia organizada en Ecuador subraya la urgente necesidad de adaptar y fortalecer los marcos normativos y las capacidades institucionales. Es fundamental enfrentar la complejidad y sofisticación de los delitos cometidos por estos grupos criminales para garantizar una administración de justicia eficaz.

Referencias bibliográficas

Albrecht, C., Duffin, K. M., Hawkins, S., & Morales Rocha, V. M. (2019). The use of cryptocurrencies in the money laundering process. Journal of Money Laundering Control, 22(2), 210-216. https://doi.org/10.1108/JMLC-12-2017-0074

Arévalo, P. A. O. (2018). El tratamiento de la evidencia digital, una guía para su adquisición y/o recopilación. Revista Economía y Política, 35-44. https://doi.org/10.25097/rep.n28.2018.03

Departamente de Seguridad de las TIC. (2023). Delitos Informáticos en Ecuador (pp. 1-9). dntic. https://www.policia.gob.ec/wp-content/uploads/downloads/2020/10/delitos-info-ecuador.pdf

Deslauriers-Varin, N., & Fortin, F. (2021). Improving Efficiency and Understanding of Criminal Investigations: Toward an Evidence-Based Approach. Journal of Police and Criminal Psychology, 36(4), 635-638. https://doi.org/10.1007/s11896-021-09491-6

Di Nicola, A. (2022). Towards digital organized crime and digital sociology of organized crime. Trends in Organized Crime. https://doi.org/10.1007/s12117-022-09457-y

DINASED. (2021). Victimología Forense: El estudio científico de las víctimas (pp. 1-84) [Gubernamental]. Policia Nacional del Ecuador. https://www.policia.gob.ec/wp-content/uploads/downloads/2021/10/Dinased-2021-7MB.pdf

Fukami, A., Stoykova, R., & Geradts, Z. (2021). A new model for forensic data extraction from encrypted mobile devices. Forensic Science International: Digital Investigation, 38, 301169. https://doi.org/10.1016/j.fsidi.2021.301169

Global Initiative Against Transnational Organized Crime. (2023). Global Organized Crime Index (pp. 1-246) [Institucional]. https://globalinitiative.net/wp-

content/uploads/2023/09/Global-organized-crime-index-2023-web-compressed-compressed.pdf

Gutiérrez Chávez, N. G. (2019). Estándar probatorio en el delito de lavado de activos y su incidencia en el debido proceso respecto a la presunción de inocencia del procesado [Tesis de maestría, Quito: Universidad Andina Simón Bolívar, Sede Ecuador]. http://repositorio.uasb.edu.ec/handle/10644/7230

Ilzan, A., Oktaviani, R., Yusuf, F., Wegman, D., Imtiyaz, N., & DedenWitarsyah. (2023). Understanding The Phenomenon and Risks of Identity Theft and Fraud on Social Media. Asia Pacific Journal of Information System and Digital Transformation, 1, 23-32. https://doi.org/10.61973/apjisdt.v101.3

Jakubiec, W. (2022). Cybercriminals and criminal structures in the world of organized crime. Scientific Journal of Bielsko-Biala School of Finance and Law, 26(4), Article 4. https://doi.org/10.19192/wsfip.sj4.2022.6

Koops, B.-J., & Leenes, R. (2020). Identity theft, identity fraud and/or identity-related crime. Datenschutz Und Datensicherheit - DuD, 30(9), 553-556. https://doi.org/10.1007/s11623-006-0141-2

Leuprecht, C., Jenkins, C., & Hamilton, R. (2022). Virtual money laundering: Policy implications of the proliferation in the illicit use of cryptocurrency. Journal of Financial Crime, 30(4), 1036-1054. https://doi.org/10.1108/JFC-07-2022-0161

Parra, D. A. P. (2022). El estándar probatorio en la medida de aseguramiento: Un análisis a partir de la Ley 1826 de 2017. Derecho Penal y Criminología, 44(116), Article 116. https://doi.org/10.18601/01210483.v44n116.05

Paucar, J. M. P., Flores, D. F. C., & Cabrita, C. M. M. (2021). La prueba digital en procesos judiciales aplicables al Código Orgánico General de Procesos (COGEP), a partir de la pandemia COVID-19. Dilemas contemporáneos: Educación, Política y Valores. https://doi.org/10.46377/dilemas.v8i.2696

Rakha, N. A. (2024). Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations. Mexican Law Review, 23-54. https://doi.org/10.22201/iij.24485306e.2024.2.18892

Saca, H., Marquez, A., & Arciniegas, C. (2024). La Inviabilidad de la Prueba Digital por Falta de Regulación en los Delitos Informáticos | 593 Digital Publisher CEIT. 8(4), 21-34. https://doi.org/10.33386/593dp.2023.4.1887

Secretaría General de INTERPOL. (2017). Estrategias sobre delincuencia organizada y nuevas tendencias delictivas (pp. 1-6) [Institucional]. INTERPOL. https://www.interpol.int/content/download/5582/file/Global%20Strategy%20on%20Organized%20and%20Emerging%20Crime-ES.pdf?inLanguage=esl-ES

Stoykova, R. (2021). Digital evidence: Unaddressed threats to fairness and the presumption of innocence. Computer Law & Security Review, 42, 105575. https://doi.org/10.1016/j.clsr.2021.105575

Wang, Z. (2020). El destino del derecho probatorio: Dos caminos de desarrollo. The International Journal of Evidence & Proof, 24(3), 329-348. https://doi.org/10.1177/1365712720930797

Wilson-Kovacs, D., Helm, R., Growns, B., & Redfern, L. (2023). Digital evidence in defence practice: Prevalence, challenges and expertise. The International Journal of Evidence & Proof, 27(3), 235-253. https://doi.org/10.1177/13657127231171620

Zabyelina, Y. (2023). Revisiting the concept of organized crime through the disciplinary lens of economic criminology. Journal of Economic Criminology, 1, 100017. https://doi.org/10.1016/j.jeconc.2023.100017

Conflicto de intereses:
Los autores declaran que no existe conflicto de interés posible.
Financiamiento:
No existió asistencia financiera de partes externas al presente artículo.
Agradecimiento:
N/A
Nota:
El artículo no es producto de una publicación anterior.