La cibercriminalidad y la legitimación de capitales

Desafíos del derecho penal internacional

Vifrán Jesús Meza Aranguren[1]
Escuela de Formación de Oficiales FAC
mezavifran@gmail.com
ORCID 0009-0004-5604-806X

Fernando Silvio Di Gerónimo[2]
Universidad Central de Venezuela
fernando.di.geronimo@gmail.com
ORCID 0009-0007-1534-6281

José Omar Pobeda Rovallo[3]
Academia Militar de la Guardia
Nacional Bolivariana
povedaroballo240783@gmail.com
ORCID 0009-0009-4648-6441

[1] Vifrán J. Meza (Venezuela), doctor en Derecho Internacional Público y en Ciencias de la Educación (ULAC); magíster en Gerencia de Seguridad Pública. Docente y consultor en aduanas, comercio exterior y cumplimiento LA/FT; formación CFCS y auditoría forense.

[2] Fernando Silvio Di Geronimo Salvatoriello (Venezuela), licenciado en Administración Pública y en Educación; doctor en Derecho Internacional Público y en Ciencias de la Educación (ULAC), con postdoctorado en DIP. Dirige Di Geronimo Real Estate y es miembro de FIABCI.

[3] José Omar Poveda Roballo (Venezuela), oficial de la GNB; comandante del Destacamento 412 de la Zona 41 Carabobo (2022–2025). Doctor en Ciencias Jurídicas, Seguridad Ciudadana y Ciencias Gerenciales; magíster en Seguridad Ciudadana y en Planificación y Conducción Operacional Militar.

La cibercriminalidad y la legitimación de capitales.

Desafíos del derecho penal internacional

Resumen

La Cuarta Revolución Industrial y la hiperconectividad han generado un ecosistema virtual propicio para delitos cibernéticos de legitimación de capitales a escala mundial. El derecho penal internacional (DPI) enfrenta el desafío de adaptarse a esta realidad transfronteriza y anónima del ciberespacio, con un catálogo de crímenes que aún no se contemplan explícitamente. Para abordar estos temas se analizan el acceso ilícito y el sabotaje de datos hasta el fraude informático, el ransomware y el malware financiero, el uso indebido de criptomonedas, la generación de flujos de "capitales sucios" y las herramientas para su blanqueo. Igualmente, se examinan las iniciativas de Venezuela y la comunidad internacional para tipificar los delitos y mejorar la cooperación para enfrentar la legitimación de capitales. Se sugieren acciones concretas para fortalecer los marcos legales existentes y agilizar la cooperación, así como continuar el debate sobre la evolución de estos temas en el derecho penal internacional.

Palabras clave: *derecho penal internacional; nuevas tecnologías; delitos cibernéticos; legitimación de capitales*

Cybercrime and Money Laundering:
Challenges for International Criminal Law

Abstract

The Fourth Industrial Revolution and hyperconnectivity have generated a virtual ecosystem conducive to cybermoney laundering crimes on a global scale. International criminal law (ICL) faces the challenge of adapting to this cross-border and anonymous reality of cyberspace, with a catalog of crimes that are not yet explicitly addressed. To address these issues, the paper analyzes everything from illicit access and sabotage of data to cyber fraud, ransomware and financial malware, the misuse of cryptocurrencies, the generation of "dirty money" flows, and the tools for laundering them. It also examines initiatives by Venezuela and the international community to define crimes and improve cooperation to combat money laundering. Concrete actions are suggested to strengthen existing legal frameworks and streamline cooperation, as well as to continue the debate on the evolution of these issues in international criminal law.

***Keywords**: International criminal law; new technologies; cybercrime; money laundering*

Introducción

La denominada Cuarta Revolución Industrial, caracterizada por la hiperconectividad, la inteligencia artificial, el cloud computing y una economía cada vez más basada en datos, ha reconfigurado de manera trascendental las dinámicas sociales y económicas a nivel global. Este nuevo paradigma, si bien ha impulsado avances sin precedentes, también ha creado un vasto ecosistema virtual que ha dado lugar a nuevos patrones y modalidades delictivas, de naturaleza fundamentalmente transnacional, conocidas como delitos cibernéticos.

Particularmente, la legitimación de capitales, un delito de naturaleza financiera, ha encontrado en el ciberespacio un medio excepcionalmente eficiente para el ocultamiento del origen ilícito de activos. A escala mundial, esta eficiencia convierte a los ciberdelitos en herramientas altamente funcionales para la delincuencia organizada y para las estructuras criminales. En este contexto, el ciberespacio funciona simultáneamente como escenario para la generación de ganancias ilícitas, a la vez que como herramienta esencial para su ocultamiento y reintegración en la economía formal, lo que ocurre tanto para los productos de crímenes convencionales como digitales. Autores como Rodríguez et al. (2017), con base en datos del Banco Interamericano de Desarrollo, aportan información precisa sobre la problemática:

Los informes de organismos internacionales y empresas vinculadas a la seguridad informática, reseñan un importante incremento de ataques cibernéticos contra personas físicas, corporaciones y gobiernos de Latinoamérica y el Caribe en el último quinquenio [...] lo que significa para las finanzas de la zona cerca de 90.000 millones de dólares anuales. (p. 64)

El derecho penal internacional (DPI), concebido históricamente para abordar crímenes de extrema gravedad como los crímenes de lesa humanidad, los crímenes de guerra y el genocidio, se enfrenta hoy a su desafío más complejo ante la irrupción del ciberespacio como un nuevo dominio de confrontación y delincuencia (Buçaj e Idrizaj, 2024). La naturaleza esencialmente transfronteriza y anónima de las actividades en línea, socava los pilares tradicionales del DPI, planteando retos significativos para su adaptación y aplicación efectiva en la era digital (Pocar, 2004).

Sobre la base de lo expuesto, este artículo se plantea como objetivo general analizar los delitos relacionados con el acceso ilícito y el sabotaje de datos digitales, así como el fraude informático, el ransomware y el malware financiero. Bajo una base metodológica de tipo cualitativa se llega a discutir, específicamente, el problema del uso indebido de criptomonedas, la generación de flujos de los denominados “capitales sucios” y las herramientas usadas para su blanqueo. Del mismo modo, el trabajo se propone examinar las iniciativas de Venezuela y la comunidad internacional para tipificar los delitos y mejorar la cooperación entre los diferentes actores, con el fin de enfrentar la legitimación de capitales. Ulteriormente, el artículo aspira contribuir a fortalecer los marcos legales existentes y agilizar la cooperación, a la vez que proporcionar ideas y reflexiones para continuar el debate sobre la evolución de estos importantes temas en el DPI. El trabajo se complementa con una nutrida selección de referencias, que enriquecen el estudio del tema.

El DPI y los delitos cibernéticos: desafíos y adaptación

La irrupción del ciberespacio ha generado una profunda tensión con los principios fundamentales del DPI. La atribución de responsabilidad individual se convierte en una tarea extraordinariamente compleja cuando los ataques utilizan redes de dispositivos comprometidos (botnets), herramientas de ofuscación como Tor o VPNs, o incluso infraestructuras de terceros países, frecuentemente con posible complicidad estatal. El anonimato en el ciberespacio es un problema fundamental, que deben enfrentar los actores que buscan garantizar la seguridad en este ámbito, por cuanto la atribución de acciones delictivas o ataques en internet son elementos ausentes en los marcos jurídicos destinados a impedir o resarcir los daños (Martabit Tellechea, 2019).

El principio de soberanía territorial, fundamental en el derecho internacional, entra en tensión directa con la realidad de un ciberataque. Un ataque lanzado desde el territorio A puede afectar infraestructuras críticas en el territorio B, transitando por servidores en los territorios C, D y E. Si bien los Estados ostentan soberanía sobre cualquier tipo de ciberinfraestructura presente en su territorio (Ríos García, 2021), la dificultad práctica para identificar el origen y la ruta de un ataque cibernético crea una paradoja. Los Estados tienen control teórico sobre su espacio digital, pero la realidad de las operaciones cibernéticas permite acciones que quebrantan la soberanía de otros sin una atribución clara, lo que obstaculiza las respuestas legales y diplomáticas efectivas.

El Estatuto de Roma de la Corte Penal Internacional no contempla, explícitamente, los delitos cibernéticos en su catálogo de crímenes. No obstante, ciertas conductas podrían subsumirse bajo figuras existentes si cumplen sus elementos constitutivos. Por ejemplo, un ciberataque masivo contra un sistema

hospitalario, que cause muertes indiscriminadas, podría configurar un crimen de guerra; o la manipulación masiva de datos esenciales para la supervivencia de una población, podría aproximarse a un crimen contra la humanidad. Esta aplicación analógica, sin embargo, genera incertidumbre jurídica. Un pilar del derecho penal es el principio de nullum crimen sine lege, que exige especificidad y claridad en la definición de los actos criminales para asegurar la certeza jurídica (Resta, 2019). Si bien la subsunción ofrece una vía pragmática para abordar nuevos ciberdelitos dentro de marcos existentes, la incertidumbre surge precisamente porque estas nuevas formas de crimen no fueron explícitamente previstas.

Los elementos del tipo penal (mens rea y actus reus), diseñados para actos físicos, pueden no alinearse perfectamente con las particularidades del daño digital. Esta dependencia de la aplicación analógica, aunque necesaria ante la ausencia de disposiciones específicas, subraya un desfase estructural fundamental en el derecho penal internacional. El marco actual es reactivo y puede tensar el principio de legalidad, lo que pone de manifiesto la necesidad urgente de un régimen jurídico más explícito y adaptado para los ciberdelitos de gravedad internacional.

En consecuencia, sigue vigente el debate sobre la necesidad de un tratado internacional específico o la inclusión de ciertos ciberataques catastróficos como crímenes internacionales autónomos. Algunos análisis académicos sugieren que los crímenes cibernéticos que amenazan la seguridad global, como el ciberterrorismo, podrían ser perseguidos bajo principios de universalidad, y los ataques a gran escala contra infraestructuras críticas podrían ser imprescriptibles (Cedeño León, et al., 2024). Sin embargo, persiste una falta de definiciones uniformes y tratados vinculantes, lo que dificulta la persecución efectiva de estos crímenes.

La persistente brecha entre el avance tecnológico criminal y la adaptación legal y regulatoria, es notoria. La naturaleza lenta, basada en el consenso de la creación de leyes internacionales, que requiere negociación, ratificación e implementación doméstica, obviamente resulta inadecuada para la evolución rápida y ágil contra las ciberamenazas. Esto genera un retraso regulatorio continuo, situación que no es meramente un inconveniente, sino que constituye una vulnerabilidad estratégica fundamental. Los actores criminales y los grupos patrocinados por ciertos Estados, explotan con relativa impunidad estas lagunas jurídicas y la ausencia de una respuesta global unificada en las zonas grises del derecho internacional (Troya Aldaz et al., 2024). Tal situación perpetúa un entorno jurídico reactivo, donde las leyes siempre están a la zaga, en lugar de disuadir proactivamente o castigar eficazmente a los ciberdelincuentes. Esta dinámica también alimenta el debate sobre la idoneidad de los dos conceptos básicos del derecho internacional, que rigen el uso de la fuerza y la conducta durante la guerra, es decir, los principios tradicionales de jus ad bellum y jus in bello para el ámbito digital (Calderón Lara, 2025; Hollis, 2020). En la figura 1, se resumen los actores clave en la lucha global contra los ciberdelitos y sus áreas de acción específicas, además de los desafíos persistentes que se deben enfrentar, los cuales merman la efectividad de sus respuestas.

Figura 1
La respuesta legal internacional

Fuente: elaboración propia

Como se puede observar diversos organismos y normativas forman la primera línea de defensa, pero enfrentan desafíos significativos para mantenerse al ritmo de la innovación criminal. Estos organismos internacionales colaboran para establecer estándares, coordinar investigaciones, cada uno con fortalezas en áreas específicas. No obstante, la efectividad afronta obstáculos estructurales, técnicos y legales.

Delitos cibernéticos como delitos precedentes de la legitimación de capitales

Los delitos cibernéticos abarcan un conjunto diverso de conductas ilícitas, donde las tecnologías de la información son el instrumento, el objetivo o el contexto del crimen (Albarrán Martínez, 2021). Este espectro es amplio y multifacético, con una conexión directa y peligrosa con la legitimación de capitales. Entre los tipos de ciberdelitos se encuentra el acceso e interferencia en sistemas, que comprende el acceso ilícito a sistemas informáticos, (conocido como “hackeo” o hacking), la interceptación fraudulenta de comunicaciones, así como el daño o sabotaje de datos y sistemas, incluyendo ataques de

denegación de servicio (DDoS) que paralizan infraestructuras críticas. También pueden citarse los delitos contra datos y contenidos, que engloban el robo masivo de datos personales o corporativos, y la explotación infantil en línea, que configuran graves violaciones de derechos fundamentales (Colorado Aguirre, 2025).

En este mismo grupo aparecen los delitos económico-financieros, con los cuales se vincula el peligro de la legitimación de capitales. Entre estos se cuentan el fraude informático, que adopta múltiples formas, como el phishing o suplantación de identidad para robar credenciales bancarias, el vishing o fraude telefónico, el Business Email Compromise (BEC), con el que se engaña a empresas para realizar transferencias fraudulentas, esquemas Ponzi digitales e inversiones falsas en criptomonedas. Otros delitos de este orden son el ransomware, que cifra datos para exigir rescates, generalmente en criptomonedas, convertido en una epidemia global extremadamente difícil de combatir (Casals Fernández, 2022), con impactos devastadores en servicios esenciales, además del malware financiero, como los troyanos bancarios, que roban directamente fondos de cuentas, mientras que la falsificación electrónica y el carding, uso de datos de tarjetas robadas, atacan el sistema financiero (Colorado Aguirre, 2025; González Uriel, 2024).

Estos delitos no solo generan enormes flujos de “capitales sucios”, sino que también proporcionan las herramientas para su blanqueo. Las ganancias del ransomware, fraude o venta de bienes ilícitos en darknets, deben ser lavadas para integrarse a la economía legítima, iniciando así un ciclo perverso donde el ciberdelito alimenta y se nutre del proceso de legitimación. Esto describe un ecosistema criminal altamente integrado y autosostenible (Broadhead, 2018). La actividad criminal inicial que es el ciberdelito, facilita y se beneficia directamente de la actividad de legitimación de capitales, la cual, al legitimar los ingresos, incentiva a su vez la comisión de más ciberdelitos.

Combatir esta dinámica, en lugar de esfuerzos aislados exige un enfoque holístico, que aborde tanto la generación de fondos ilícitos como los mecanismos para su blanqueo (Cano y Monsalve, 2023). Interrumpir una parte del ciclo puede tener un efecto cascada en la otra, lo que subraya la importancia de estrategias coordinadas.

A continuación, se presenta en la tabla 1 el resumen de la tipología de ciberdelitos y sus vínculos con la legitimación de capitales.

Tabla 1

Tipología de ciberdelitos y su vínculo con la legitimación de capitales

Tipo de ciberdelito (Categoría principal)	Ejemplos específicos	Mecanismo de generación de capital ilícito	Vínculo con la legitimación de capitales (delito precedente)
Delitos contra sistemas informáticos	Acceso ilícito (hacking) sabotaje/daño a datos, ataques DDoS, interferencia en sistemas.	Acceso a información para venta, interrupción de servicios para extorsión, destrucción de datos para chantaje.	Genera fondos que requieren blanqueo; puede destruir rastros de transacciones.
Delitos financieros cibernéticos	Fraude informático (phishing, vishing, BEC, esquemas Ponzi digitales), ransomware, malware financiero, falsificación electrónica, carding.	Robo directo de fondos bancarios/credenciales, extorsión por secuestro de datos, engaño para transferencias fraudulentas, uso de datos de tarjetas robadas.	Genera enormes volúmenes de fondos ilícitos que necesitan ser blanqueados; el rescate de ransomware a menudo se exige en criptomonedas.
Delitos de contenido	Pornografía infantil online, difusión de contenidos ilícitos.	Venta de material ilegal, explotación de víctimas para ganancias.	Los fondos obtenidos de estas actividades requieren blanqueo para integrarse en la economía formal.
Delitos contra la propiedad intelectual	Piratería de software, difusión ilícita de archivos protegidos.	Venta de copias ilegales de software, música, películas.	Los ingresos de la venta de productos piratas son ilícitos y deben ser blanqueados.
Delitos de privacidad y datos personales	Robo masivo de datos personales o corporativos, ciberespionaje.	Venta de bases de datos robadas, información confidencial para extorsión o ventaja competitiva.	Los datos robados pueden ser monetizados, generando fondos que requieren legitimación.

Fuente: Elaboración propia a partir de documentos

La legitimación de capitales en la era digital: Nuevas técnicas y desafíos

En la era digital el blanqueo de capitales ha evolucionado significativamente, trascendiendo el tradicional modelo trifásico de colocación, estratificación e integración. Las nuevas tecnologías permiten una fusión y aceleración de estas etapas, con lo que hacen el proceso más rápido y opaco (Suganya Arawazhi, 2020).

La fase de colocación, que implica la introducción inicial de fondos ilícitos en el sistema financiero, en estos tiempos puede producirse mediante depósitos en cajeros automáticos con tarjetas prepago robadas, el uso de exchanges de criptomonedas sin controles efectivos de "Conozca a su Cliente" (KYC), o microtransacciones en las llamadas "cuentas mula".

La estratificación, fase que usualmente sigue en este proceso, tiene la finalidad de difuminar el rastro del dinero. Esta fase resulta potenciada por las criptomonedas, que ofrecen seudonimato, lo que implica que, si bien no hay un anonimato total, sí existe un alto grado de opacidad, lo cual permite transferencias transfronterizas instantáneas (Casals Fernández, 2022; Cedeño León et al., 2024; Hinojal, 2024; Pérez Medina, 2020; Ríos García, 2021).

Dichas características crean una "trampa de seudonimato" para los investigadores. Aunque las transacciones se registran en una cadena de bloques pública, vincular estas direcciones seudónimas a individuos o entidades del mundo real, representa un obstáculo importante para los investigadores. Aunque no es una imposibilidad técnica, requiere herramientas y experiencia especializadas, como forenses digitales y análisis de blockchain, entre otras (Pérez Medina, 2020; 2004; Rada, 2024; Wu et al., 2020) y a menudo cooperación transfronteriza, que suele ser lenta o muy complicada (Pocar, 2004).

La dificultad práctica y los muchos recursos necesarios para desanonimizar estas transacciones, proporcionan un escudo efectivo para los criminales, lo que exige un cambio en los paradigmas de investigación y una inversión considerable en capacidades, más allá de la inteligencia financiera tradicional (Pocar, 2004; Wu et al., 2020). Para la estratificación, los delincuentes utilizan diversas técnicas, tales como el movimiento rápido de fondos entre múltiples carteras (wallets), el uso de exchanges en jurisdicciones con regulaciones laxas, servicios de mezcla (mixers o tumblers), que combinan criptomonedas de múltiples usuarios y criptomonedas privadas y descentralizadas. Los mixers agrupan fondos de múltiples usuarios, dificultando el rastreo de transacciones individuales (Hinojal, 2023). A este complejo proceso de estratificación digital, se agregan los servicios de pago en línea con billeteras electrónicas, o sistemas P2P, el comercio electrónico ficticio con tiendas en línea falsas, que simulan ventas y técnicas de ofuscación de red (VPN, Tor, etc.).

Como última fase, la integración se realiza cada vez más en la propia economía digital: inversión en criptoactivos volátiles, compra de bienes digitales como NFTs o dominios web valiosos, o inversión en startups tecnológicas. Esta sofisticación convierte al ciberespacio en un conducto ideal no solo para generar ganancias ilícitas, sino para transformarlas en aparentemente legítimas (Hinojal, 2023).

El crecimiento acelerado y la adopción generalizada de los activos digitales, así como la economía digital en general, ofrecen nuevas vías, menos escrutadas, para los blanqueadores de capitales. Lo que antes se consideraba una inversión de nicho o especulativa, es ahora una parte significativa del panora-

ma financiero global. La percepción de legitimidad y las rápidas fluctuaciones de valor de ciertos activos digitales, combinadas con una supervisión regulatoria menos madura en comparación con las finanzas tradicionales, los convierten en vehículos atractivos para integrar fondos ilícitos. La apariencia legítima de estas inversiones digitales, dificulta su diferenciación de la actividad económica genuina (Pérez Medina, 2020).

Esta tendencia implica que los esfuerzos de lucha contra el blanqueo de capitales y la financiación del terrorismo, ya no pueden centrarse exclusivamente en las instituciones financieras tradicionales. Los reguladores y las fuerzas del orden deben ampliar su ámbito de acción a todo el ecosistema de activos digitales, incluyendo las formas emergentes de valor digital como los NFTs y las plataformas que facilitan su intercambio (Suganya Arawazhi, 2020). Se requiere el desarrollo de nuevas metodologías de detección y marcos legales que puedan seguir el ritmo de la evolución de la economía digital, a fin de evitar que se convierta en conducto principal para la riqueza ilícita.

Instrumentos y cooperación internacional en la lucha contra el cibercrimen y la legitimación de capitales

El Convenio de Budapest

La comunidad internacional, aunque con limitaciones significativas, ha desarrollado diversos instrumentos para enfrentar la convergencia entre el cibercrimen y la legitimación de capitales. Entre dichos instrumentos destaca el Convenio de Budapest, promulgado en la capital magiar el 23 de noviembre de 2001, constituye el principal tratado internacional en esta materia. En el preámbulo de este documento se reconoce la necesidad de emplear, prioritariamente, "una política penal común, con objeto de proteger a la sociedad frente a la ciberdelincuencia, en particular mediante la adopción de una legislación adecuada y la mejora de la cooperación internacional". A la vez se expresa preocupación por el riesgo de que "las redes informáticas y la información electrónica sean utilizadas (...) para cometer delitos y de que las pruebas relativas a dichos delitos sean almacenadas y transmitidas por medio de las redes". Ante tales riesgos, se estima indispensable la "cooperación entre los estados y el sector privado en la lucha contra la ciberdelincuencia" y se subraya la necesidad "de proteger los intereses legítimos en la utilización y el desarrollo de las tecnologías de la información" (Consejo de Europa, 2001, p. 1).

El referido Convenio establece estándares mínimos para la tipificación de delitos informáticos como acceso ilícito, interceptación, daño a datos, fraude informático, entre otros, y crea mecanismos de cooperación en investigación, tales como preservación de datos, asistencia mutua y extradición, etc. (Díaz Gómez, 2010). A lo largo de los años, el Convenio ha sido revisado y actualizado para adaptarse a la evolución de las tecnologías, garantizando de esta manera la continuidad

de su relevancia y eficacia, además de que se proyectan sus posibles implicaciones a futuro (Calderón Lara, 2025; Gonzalo Pastrana, 2013; Gertler, 2024).

Sin embargo, el alcance del Convenio es limitado, puesto que no aborda explícitamente el vínculo con el blanqueo de capitales, ni regula adecuadamente las criptomonedas, además de que su ratificación no es universal, lo que deja vacíos jurisdiccionales (Díaz Gómez, 2010). Esto obedece a que el Convenio fue firmado en 2001, precede a la adopción masiva de criptomonedas y las sofisticadas técnicas de blanqueo digital.

A pesar de las revisiones, un tratado redactado antes de la aparición plena de un fenómeno como el blanqueo de capitales, facilitado por criptomonedas, indudablemente tendrá dificultades para proporcionar herramientas legales precisas y completas, por lo que su adaptación deberá ser progresiva. El Convenio de Budapest, aunque fundamental y exitoso en establecer una base para la legislación sobre ciberdelitos, funciona como un documento heredado en el contexto del crimen financiero digital avanzado. Sus limitaciones resaltan la necesidad crítica de un nuevo instrumento internacional más completo, que aborde específicamente el nexo entre el cibercrimen y el blanqueo de capitales, y los activos virtuales, o bien un mecanismo de actualización rápido y significativo para los tratados existentes, a fin de evitar que queden obsoletos frente a la aceleración de la innovación tecnológica y criminal (Merino Ajila, 2024; Pons, 2017).

El Grupo de Acción Financiera Internacional (GAFI/FATF), sus recomendaciones clave y su implementación

Para los mismos fines generales relacionados con el Convenio de Budapest, el Grupo de Acción Financiera Internacional (GAFI/FATF) desempeña un papel crucial a través de sus Recomendaciones, que constituyen el estándar global contra el lavado de activos y el financiamiento del terrorismo (LA/FT) (Meza Aranguren, 2024; Pavlidis, 2020). Específicamente, la Recomendación 15 del GAFI exige que países e instituciones identifiquen y mitiguen los riesgos asociados a nuevas tecnologías, incluyendo activos virtuales en criptomonedas y sus proveedores de servicios. Esta recomendación obliga a regular, licenciar o registrar, y monitorear efectivamente a los Proveedores de Servicios de Activos Virtuales (VASP, por sus siglas en inglés) (Pavlidis, 2020). El enfoque basado en riesgo (EBR) obliga a aplicar medidas de debida diligencia mejorada (EDD) proporcionales al riesgo.

La Recomendación 16, conocida como Travel Rule, es particularmente relevante ya que obliga a los VASP a compartir información del originador y beneficiario en transacciones de criptomonedas como nombre, dirección, o datos de cartera; similar a lo requerido en transferencias bancarias tradicionales. Su implementación técnica en el ecosistema cripto es compleja pero esencial para rastrear flujos ilícitos. Para su empleo se requieren la interoperabilidad, por cuanto no hay una única solución o protocolo, sino múltiples opciones; la protección de datos, de los que hay que compartir identificaciones sensibles de clientes entre jurisdicciones con leyes variables; el problema conocido como del sunrise issue, que se refiere a la adopción global desigual de la Travel Rule, entre otros procesos (Takei y Shudo, 2024).

Las recomendaciones del GAFI, aunque son estándares globales, representan en última instancia directrices que los países deben convertir en ley. Desde luego, el proceso está sujeto a prioridades legislativas nacionales, voluntad política e interpretaciones diversas de la protección de datos y la soberanía. Esta situación conduce a una falta de armonización regulatoria global. Cuando algunas jurisdicciones implementan controles estrictos, como la Travel Rule, y otras no lo hacen, o lo hacen con menor rigor, se crean oportunidades para el arbitraje regulatorio. Los criminales pueden simplemente trasladar sus maniobras a jurisdicciones menos exigentes, socavando la eficacia del estándar global. El éxito de los esfuerzos globales contra el lavado de activos y la financiación del terrorismo, concretamente en el ámbito de los activos virtuales, no depende solo de la existencia de recomendaciones sólidas, sino de su implementación uniforme y rigurosa en todas las jurisdicciones importantes. El enfoque fragmentado actual, impulsado por la discreción soberana y las capacidades técnicas variables, crea inadvertidamente refugios seguros para los flujos financieros ilícitos, lo que exige un impulso más fuerte hacia la armonización legal y técnica internacional (Díaz, Gómez, 2010; González Pastrana, 2013; Pavlidis, 2020).

El papel de Interpol y Europol en la cooperación operativa

Organismos como Interpol y Europol, a través de su Centro Europeo de Ciberdelincuencia, EC3, facilitan el intercambio de inteligencia, apoyo técnico y operaciones conjuntas. Interpol tiene un alcance general con 195 países miembros, gestiona una red global de intercambio de información y publica las denominadas Red Notices, notificaciones emitidas para lograr la localización y detención de un presunto delincuente, solicitado por alguna jurisdicción judicial o un tribunal internacional. Europol, por su parte, se centra en la lucha contra la delincuencia

transnacional y el terrorismo dentro de la Unión Europea, proporcionando apoyo analítico y coordinando Equipos Conjuntos de Investigación (JIT), aunque carece de poder para realizar arrestos. Las redes de puntos de contacto 24 horas por siete días a la semana, permiten respuestas rápidas a incidentes transfronterizos (Reedy, 2020).

A pesar de estos instrumentos, persisten los desafíos debido a las diferencias en los marcos legales nacionales, la lentitud en los procesos de asistencia mutua legal, así como a las desiguales capacidades técnicas entre los diferentes países. A lo anterior se suma la constante innovación de los delincuentes, quienes explotan las nuevas tecnologías más rápidamente de lo que pueden hacerlo las respuestas regulatorias. Por otra parte, la recuperación transnacional de activos, como acción fundamental contra la corrupción de cualquier índole, es un proceso intrincado, que requiere una permanente cooperación internacional, eficientemente instrumentada (Abreu Valencia, 2022). Como lo señala Varela (2024), “el mecanismo de recuperación de activos es actualmente entendido como uno de los principales bastiones para combatir la corrupción, dado su eficaz efecto demoledor de algunos de los eslabones de la cadena criminal” (Párr. 11).

El marco legal venezolano: la Ley Especial contra los Delitos Informáticos (LEDI) y la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT)

Venezuela cuenta con un marco legal que, en teoría, aborda tanto los delitos cibernéticos como su vínculo con la legitimación de capitales (Meza Aranguren, 2024). En el artículo 1, la Ley Especial contra los Delitos Informáticos (LEDI), expresa que tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías (Asamblea Nacional de la República Bolivariana de Venezuela, 2001).

Dicho instrumento legal tipifica una amplia gama de conductas delictivas y clasifica los delitos en cinco grupos principales: contra los sistemas que utilizan tecnologías de información, contra la propiedad, contra la privacidad de las personas y de las comunicaciones, contra niños y adolescentes, y contra el orden económico. Entre los delitos específicos tipificados se encuentran el acceso indebido, el sabotaje o daño a sistemas, la posesión de herramientas para delitos informáticos, el espionaje, la falsificación electrónica, el fraude mediante tecnologías y la pornografía infantil. La LEDI concibe como bienes jurídicos protegidos los sistemas informáticos que contienen, procesan, resguardan y transmiten la información (Asamblea Nacional de la República Bolivariana de Venezuela, 2001).

Por otra parte, la Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo (LOCDOFT) (Asamblea Nacional de la República Bolivariana de Venezuela, 2012) define el delito de legitimación de capitales de manera amplia e incluye expresamente los delitos tipificados en la LEDI como delitos precedentes. La LOCDOFT también establece clara-

mente, como circunstancia agravante para los delitos previstos en la Ley, el uso de medios informáticos que alteren los sistemas de información de las instituciones del Estado. El objetivo de la ley es prevenir y controlar la legitimación de capitales, el financiamiento al terrorismo y el financiamiento de armas de destrucción masiva.

Tendencias y desafíos prácticos en Venezuela

En la práctica venezolana, se observan tendencias que destacan el nexo entre ciberdelitos y legitimación de capitales (Meza Aranguren, 2024; Rodríguez, 2016). Proliferan los fraudes masivos en línea, especialmente esquemas Ponzi (fraude de inversión que opera pagando a los inversores existentes con el dinero de nuevos inversores) y de inversiones falsas promovidos en redes sociales, así como ataques de phishing dirigidos a usuarios de banca en línea. El ransomware afecta a empresas e instituciones públicas, aunque su reporte oficial es escaso. Los fondos provenientes de la corrupción, el narcotráfico y la minería ilegal, junto con presumibles ganancias de ciberdelitos, son convertidos a criptomonedas en exchanges locales o internacionales, con controles débiles. Posteriormente, son estratificados mediante mixers o transferencias múltiples entre carteras, antes de ser integrados en la economía formal o convertidos a divisas fuertes en el exterior.

La situación en Venezuela revela una brecha entre la existencia de un marco legal y su eficacia práctica. La mera existencia de legislación es insuficiente sin las capacidades de aplicación sólidas, que incluyen forenses digitales especializados, una supervisión regulatoria proactiva de los activos digitales y una cooperación internacional efectiva para abordar los flujos transfronterizos (Rodríguez, 2016). Los controles laxos en los exchanges son una vulnerabilidad crítica que desgasta las disposiciones legales internas. Esta situación sirve para estudiar

los casos del desafío global común: la brecha entre las disposiciones legales de jure y la aplicación de facto (Rodríguez et al., 2017).

Sobre estos problemas, Torres (2018) subraya que las estrategias efectivas contra el cibercrimen y el lavado de activos requieren no solo previsión legislativa, sino también una inversión significativa en capital humano, como investigadores y fiscales capacitados, herramientas tecnológicas y voluntad política para aplicar rigurosamente la ley y participar en la colaboración internacional.

Debate sobre el artículo 51 de la Carta de la ONU y ciberataques

La definición de lo que constituye un ataque armado, bajo el Artículo 51 de la Carta de la ONU, se torna ambigua cuando el daño es causado por un código malicioso en lugar de armas convencionales (Naciones Unidas, 2025). Las discusiones académicas exploran cómo el derecho internacional se aplica a las operaciones cibernéticas, incluyendo el principio de soberanía y no intervención (Hollis, 2020). Algunos Estados consideran medidas de retorsión en respuesta a operaciones cibernéticas ilícitas u hostiles, incluso si no violan el derecho internacional. Sin embargo, hasta 2020, ningún Estado había tomado formalmente contramedidas contra otro Estado en respuesta a un ciberataque, lo que sugiere una reticencia a clasificarlos como actos internacionalmente ilícitos que justifiquen tales respuestas (Piernas López, 2024).

El dilema del umbral de la fuerza en la ciberguerra es una brecha crítica en el derecho internacional. Los ciberataques pueden causar daños ingentes, como paralizar infraestructuras vitales, sin implicar fuerza física o destrucción física directa. El debate se centra en cuál nivel de daño inducido por un

ciberataque cruza el umbral, para ser considerado un ataque armado que justifique la legítima defensa. La falta de consenso y la reticencia de los Estados a etiquetar formalmente los ciberataques como actos internacionalmente ilícitos, indican esta ambigüedad (Broadhead, 2018; Cano y Monsalve, 2023). Los Estados pueden dudar en responder con fuerza a ciberataques graves, por temor a violar el derecho internacional o a escalar conflictos, mientras que los agresores explotan esta ambigüedad para operar por debajo del umbral tradicional de guerra. Esto exige un diálogo multinacional urgente y la construcción de consenso para clarificar la aplicación del jus ad bellum en el ámbito digital, lo que podría conducir a nuevas normas o interpretaciones (Buçaj e Idrizaj, 2024; Martabit Tellechea, 2019; Pocar, 2004).

En síntesis, queda clara la urgencia de considerar algunos ciberataques graves como crímenes internacionales, más allá de su subsunción bajo categorías existentes, como crímenes de guerra o crímenes de lesa humanidad. Igualmente, es importante destacar que el uso de herramientas de vigilancia masiva para prevenir ciberdelitos, plantea dilemas éticos significativos. Es de la mayor relevancia garantizar que estas herramientas respeten los derechos fundamentales, como la privacidad y la libertad de expresión. Tal como lo asevera Floridi (2019), desconocer estos principios puede ser la fuente de muchos males, de ello se infiere que la solución suele comenzar por más y mejor información para todos los actores (p. 192).

Conclusiones y recomendaciones

La ciberdelincuencia abarca no solo los delitos contra los sistemas informáticos, sino también los delitos cometidos mediante cualquier tecnología que permita el procesamiento e intercambio de información. Este tema, desde hace varios años ha estimulado e interesado a profesionales y a teóricos de la justicia penal. Su dimensión internacional y la constante evolución tecnológica, hacen que este campo sea particularmente importante y complejo. El segundo de los rasgos citados, implica el riesgo de que cualquier respuesta regulatoria sea insuficiente para abordar los avances en nuevas técnicas y prácticas de intrusión, en diversos sistemas de comunicación digital. En la actualidad, es difícil siquiera imaginar ejemplos de ciberdelincuencia con una dimensión meramente nacional; muchas actividades delictivas pueden cometerse ahora en cualquier lugar y tener efectos inmediatos en muchos otros países, gracias al abuso de los sistemas de telecomunicaciones y de las redes informáticas.

La peligrosa sinergia entre los delitos cibernéticos y la legitimación de capitales, representa una de las amenazas más dinámicas y complejas, tanto para la seguridad global como para la integridad de los sistemas financieros. Las nuevas tecnologías actúan como un catalizador, multiplicando la escala, la velocidad y la opacidad de estas actividades ilícitas. El DPI, aunque en proceso de adaptación, lucha contra su permanente desfase frente a la innovación criminal.

Los desafíos persistentes incluyen el anonimato y la atribución de responsabilidad, que continúan siendo imponentes obstáculos para la persecución efectiva. Las complejidades jurisdiccionales y las diferencias en los marcos legales nacionales, impiden una aplicación transfronteriza eficaz. La rápida evolución de las tácticas criminales supera constantemente las respuestas regulatorias y legislativas. Además, la necesidad

de capacidades forenses digitales consistentes y una asistencia mutua legal son primordiales, pero a menudo deficientes. El desfase entre la legislación existente y la capacidad de aplicación efectiva sigue siendo un punto crítico.

La respuesta a estos delitos depende, en gran medida, del funcionamiento de los mecanismos de cooperación entre las distintas autoridades nacionales, que deben ser especialmente eficaces para abordar la rapidez de los flujos de información y la volatilidad de los datos transmitidos. Sin embargo, al examinar la legislación internacional, se observa que los instrumentos de cooperación judicial aún ofrecen procedimientos rígidos, que tienden a ser lentos y laboriosos, lo que a menudo los torna inadecuados para garantizar una rápida coordinación de las iniciativas emprendidas a nivel nacional. Las innovaciones introducidas, por ejemplo, por el citado Convenio de Budapest, no parecen ser suficientes para que las autoridades judiciales puedan actuar con la misma rapidez que los ciberdelincuentes. La situación se complica aún más por la existencia de lo que se define como un sistema multicapa, el cual se basa en la premisa de:

> *«Ningún mecanismo de defensa es infalible. Usando varias capas de defensa, una organización puede protegerse contra una serie más amplia de amenazas y minimizar el potencial de un solo punto de falla. Este enfoque implica la implementación de múltiples medidas de seguridad en diferentes niveles para proteger la red, los endpoints, los usuarios y los datos de una organización contra las ciberamenazas. (Arnal, 2023, párr. 2)»*

Esto significa que la respuesta a la ciberdelincuencia no puede basarse únicamente en la cooperación tradicional entre autoridades judiciales nacionales similares, es decir, aquellas con la misma naturaleza y competencia, que operan en procesos penales. El uso de sistemas de telecomunicaciones y redes informáticas requiere obtener información en poder de diversas entidades con objetivos, naturaleza y competencias muy diferentes. Esto incluye, por ejemplo, a las autoridades administrativas, pero también a actores privados que desempeñan un papel cada vez más importante en la respuesta a la ciberdelincuencia. De hecho, los proveedores de estos servicios de telecomunicaciones tienen acceso privilegiado a los datos solicitados por las autoridades judiciales, por lo que su cooperación es indispensable.

Para enfrentar la compleja amenaza que representa la convergencia del cibercrimen y la legitimación de capitales, son recomendables acciones concretas, implementadas a diferentes niveles. Entre ellas destaca el fortalecimiento de marcos legales y la promoción de la ratificación universal de tratados. Con relación a este aspecto, es imperativo fortalecer la ejecución del Convenio de Budapest y promover su ratificación universal, a fin de ampliar su alcance jurisdiccional (Consejo de Europa, 2001; Hertler, 2024). Se debe explorar la viabilidad de nuevos instrumentos internacionales o enmiendas significativas a los existentes, que aborden explícitamente el nexo entre el cibercrimen y la legitimación de capitales, así como los desafíos específicos planteados por los activos virtuales (Buçaj e Idrizaj, 2024).

Para los mismos propósitos, debe mejorarse la implementación de esquemas internacionales y el monitoreo riguroso de su aplicación. Los estándares del GAFI, particularmente la Recomendación 15 y la Travel Rule, deben aplicarse rigurosamente por todos los Estados miembros, con un monitoreo mejorado y la definición de sanciones para el incumplimiento.

Acerca de las medidas legislativas recomendadas, resalta la necesidad de que estas contemplen otorgar suficiente autoridad con el propósito de rastrear, identificar y cuantificar bienes sujetos a decomiso. Potestades que deben contemplar también la ejecución de medidas provisionales, como el congelamiento y el embargo, con el propósito de prevenir cualquier manejo de los bienes en cuestión. Del mismo modo, las autoridades deberán tener la facultad de adoptar medidas que imposibiliten o anulen acciones que puedan comprometer la capacidad del Estado para incautar bienes sujetos a decomiso, incluyendo la apertura de los procesos de investigativos pertinentes (Meza Aranguren, 2024).

Por otra parte, las exigencias que sobrevienen a causa de la operación conjunta y de la protección de datos en la implementación de la Travel Rule, deben abordarse mediante protocolos técnicos estandarizados y acuerdos internacionales sobre el intercambio de datos (Pavlidis, 2020).

Igualmente, debe considerarse de la mayor importancia la agilización de la cooperación operativa y el desarrollo de capacidades forenses digitales. La cooperación debe agilizarse mediante canales de intercambio más ágiles y equipos conjuntos de investigación (JIT) con capacidades técnicas reforzadas. Las redes de puntos de contacto 24/7 deben utilizarse y fortalecerse plenamente, a fin de asegurar respuestas rápidas a incidentes transnacionales. Es crucial apoyar el desarrollo de capacidades forenses digitales y de análisis financiero en los países con menos recursos, incluyendo capacitación y acceso a herramientas avanzadas (Rada, 2024; Wu et al., 2024).

Se recomienda también la continuación el estudio, las reuniones y convenciones para decidir los cambios y la evolución del derecho penal internacional, que incluya como crímenes serios los delitos provocados por el uso de las nuevas tecnologías. El objetivo es lograr claridad jurídica y consenso sobre

el denominado umbral de la fuerza en el ciberespacio. Debe recordarse, -en una época y en un mundo convulsionado por las guerras- que aún no existen criterios internacionalmente aceptados para determinar si un ciberataque perpetrado por un Estado-nación constituye un uso de la fuerza equivalente a disparos, bombas o proyectiles de guerra, lo que podría desencadenar una respuesta militar. Asimismo, todavía no se han redactado instrumentos internacionales jurídicamente vinculantes, que regulen explícitamente las relaciones interestatales en el ciberespacio (Calderón Lara, 2025; Merino Ajila, 2024).

El derecho internacional permite la legítima defensa y las medidas contra ataques armados, cuando un beligerante viola el derecho internacional en tiempo de paz o el derecho de los conflictos armados en tiempo de guerra. Sin embargo, los ciberataques siguen sin una definición final (Resta, 2019). Además, persisten las dudas sobre cuáles disposiciones del derecho internacional vigente podrían regir la conducción de una guerra entre naciones que se vean realmente impactadas por graves daños en el ciberespacio.

Del mismo modo, se considera relevante fomentar una decidida colaboración entre el sector público con las fuerzas del orden y las instituciones reguladoras en conjunto con la industria privada cuyas empresas de tecnología, instituciones financieras, empresas de ciberseguridad están siendo impactadas por los delitos cibernéticos y la legitimación de capitales. Su unión permitirá compartir información de inteligencia, desarrollar mejores prácticas y contribuir a desarticular operaciones criminales. Así mismo, se deben promover campañas de concienciación y educación pública sobre ciberseguridad y riesgos de fraude financiero, para mejorar la prevención y la resiliencia.

Los resultados de las investigaciones demuestran que los programas educativos integrales reducen significativamente la probabilidad de delitos cibernéticos, al promover un comportamiento responsable en línea, aumentar el conocimiento de las

amenazas cibernéticas y equipar a los usuarios con destrezas de protección (Kudratov, 2025). Finalmente, se debe alentar el desarrollo de un paradigma regulatorio proactivo y adaptable, que pueda anticipar y responder a las amenazas emergentes, en lugar de reaccionar únicamente a los patrones criminales ya establecidos.

Con base en lo anterior, se enfatiza en la conveniencia de incorporar conocimientos relacionados con la seguridad informática en los programas educativos de todos los niveles. Los niños y niñas deberían aprender a evitar las trampas de los pedófilos y comprender que la última versión de algún juego en línea no es lo más conveniente para su educación. Los estudiantes de secundaria deberían estar en capacidad de reconocer un intento de phishing, (Kudratov, 2025) cuáles datos personales se pueden compartir públicamente en las redes sociales, de forma segura, y qué información debe mantenerse confidencial (Suganya Arawazhi, 2020).

Igualmente, todos los usuarios deberían estar en condiciones de entender la configuración predeterminada de los equipos, así como sus riesgos, aunque no les sea posible modificar los archivos de configuración (Arreola, 2019); sin embargo, deberían ser conscientes de tales riesgos y proceder en consecuencia, inclusive incorporando a sus actividades la práctica de consultar con especialistas cuando tengan dudas o se les presente algún problema.

Todos los usuarios de la tecnología de la información deberían poder reconocer cuándo un hacker intenta acceder a un sistema, lo que puede ser útil para el usuario también porque estará mejor preparado, con ciertas medidas protectoras como antivirus, firewall, configuraciones más seguras, etc., a la vez que le ayudará a reconocer un ataque y actuar en consecuencia. Cabe recordar que, con relación a los riesgos inherentes al uso de los recursos digitales en la comunicación, la llamada

Teoría de las Actividades Rutinarias (TAR), destaca tres factores fundamentales: delincuente motivado, objetivo adecuado y falta de vigilancia eficaz (Rodríguez et al, 2017, p. 73). Una educación apropiada en este campo, con la mayor certeza tendría un efecto disuasivo y, en alguna medida, redundaría en la lucha contra el cibercrimen.

Llegar a legitimar capitales producto de los delitos cibernéticos tiene una mixtura de componentes que incluyen el conocimiento de las debilidades de los grupos sociales, las oportunidades de la aplicación de tecnologías sin controles y la ausencia de consenso en el ámbito global. El verdadero combate contra estos crímenes se podrá adelantar con la decisión de actualización y aplicación de nuevas leyes en el derecho penal internacional.

Referencias

Abreu Valencia, F. (2022). La cooperación internacional en materia de cibercrimen y evidencia digital. Saber y justicia, 1(21), 30-53 https://dialnet.unirioja.es/servlet/articulo?codigo=8500602

Albarrán Martínez, E. E. (2021). Delitos cibernéticos. Transregiones. Revista de Estudios Sociales y Culturales, (2), 93-104. https://revistatransregiones.com/web/index.php/tr/article/view/18

Arnal, C. (2023). Fortalecimiento de la seguridad: el poder de múltiples capas contra amenazas avanzadas. WatchGuard. https://www.watchguard.com/es/wgrd-news/blog/fortalecimiento-de-la-seguridad-el-poder-de-multiples-capas-contra-amenazas-0

Arreola, A. (2019). Ciberseguridad ¿Por qué es importante para todos? Siglo XXI Editores.

Asamblea Nacional de la República Bolivariana de Venezuela. (2001). Ley Especial contra los Delitos Informáticos. Gaceta Oficial de la República Bolivariana de Venezuela No. 37.313.

Asamblea Nacional de la República Bolivariana de Venezuela. (2012). Ley Orgánica contra la Delincuencia Organizada y Financiamiento al Terrorismo. Gaceta Oficial de la República Bolivariana de Venezuela No. 39.912.

Broadhead, S. (2018). The contemporary cybercrime ecosystem: A multi-disciplinary overview of the state of affairs and developments. Computer Law & Security Review, 34(6), 1.189-1.196. https://doi.org/10.1016/j.clsr.2018.08.005

Buçaj, E. e Idrizaj, K. (2024). The need for cybercrime regulation on a global scale by the international law and cyber convention. Multidisciplinary Reviews, 8(1), 1-10. https://doi.org/10.31893/multirev.2025024

Calderón Lara, N. (2025). El ciberespacio como escenario de conflicto en el siglo XXI. ¿hacia la militarización de la ciberseguridad? Razón Crítica, (18), 1-21. https://doi.org/10.21789/25007807.2110

Cano, W. D. y Monsalve, S. (2023). Ciberseguridad, reto empresarial para afrontar la era de la digitalización actual [Tesis de grado]. Universidad Pontificia Bolivariana. http://hdl.handle.net/20.500.11912/11318.

Casals Fernández, Á. (2022). Las criptomonedas frente al delito de blanqueo de capitales y la complejidad de la prueba pericial en el ámbito ciberdelincuente. Anuario de Derecho Penal y Ciencias Penales, (75), 421-446. http://hdl.handle.net/10637/14727.

Cedeño León, J., Sánchez Erazo, A., Lemos Espinoza, A., Quito Carpio, C., Fuentes Tenorio, E. y Jiménez Guartán, J. (2024). Crímenes cibernéticos como nuevas formas de delitos internacionales: retos para el derecho penal internacional. Polo del Conocimiento. Revista Científico-Académica Multidisciplinaria, 9(12), 2203-2212. https://doi.org/10.23857/pc.v9i12.8613

Colorado Aguirre, R. (2025). Delitos cibernéticos y la protección de datos personales en la era digital. Polo del Conocimiento. Revista Científico-Académica Multidisciplinaria, 10(6), 2352-2365. https://doi.org/10.23857/pc.v10i6.9818

Consejo de Europa. (2001). Convenio sobre la ciberdelincuencia. Serie de Tratados Europeos No. 185. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Díaz Gómez, A. (2010). El delito informático, su problemática y la cooperación internacional como paradigma de su solución: El Convenio de Budapest. Revista Electrónica de Derecho de la Universidad de la Rioja (REDUR), (8), 169-203. https://doi.org/10.18172/redur.4071

Floridi, L. (2019). Translating principles into practices of digital ethics: Five risks of being unethical. Philosophy & Technology, 32(2), 185-193. https://doi.org/10.1007/s13347-019-00354-x

González Pastrana, A. (2013). Lucha contra la ciberdelincuencia en la Unión Europea: creación del Centro Europeo de Ciberdelincuencia. Seguridad y Ciudadania. Revista del Ministerio del Interior, (9), 15-62. https://www.interior.gob.es

González Uriel, D. (2024). Algunas dificultades en la detección e investigación de los ciberdelitos económicos. Ciencia Policial, (183), 181–224. https://doi.org/10.14201/cp.32207

Hertler, F. E. (2024). Ciberdelitos 2024: El Convenio de Budapest y su influencia en el derecho penal argentino. Nueva Crítica Penal, 6(11), 16-59. http://revista.criticapenal.com.ar/index.php/nuevacriticapenal/article/view/89

Hinojal, A. (2023). Criptomonedas y blanqueo de capitales. Logos Guardia Civil, Revista Científica del Centro Universitario de la Guardia Civil, (1), 215-240. https://revistacugc.es/article/view/5742

Hollis, D. (2020). Derecho Internacional y operaciones cibernéticas del Estado: Mejora de la transparencia. (OEA/Ser. Q CJI/doc. 603/20 rev. 1; Cuarto informe). Organización de los Estados Americanos. http://www.oas.org/es/sla/cji/docs/temas_culminados _recientemente_derecho_internacional_operaciones_ciberneticas_estado_INFORME_FINAL.pdf

Kudratov, A. N. (2025). The Role of Education in Preventing Cybercrime. Solving Social Problems in Management and Economics, 4(6), 19-21. https://inlibrary.uz/index.php/sspme/article/view/86328

Martabit Tellechea, P.(2019). Atribución en el ciberespacio: piedra tope en el derecho internacional. Cuaderno de Trabajo del Centro de Investigaciones y Estudios Estratégicos, (14), 1-18. https://anepe.cl/wp-content/uploads/2020/10/Cuaderno-de-Trabajo-N%C2%B014-2019.pdf

Merino Ajila, F. (2024). Evolución Internacional de la Legislación sobre Ciberdelincuencia Tras el Convenio de Budapest. Ciencia Latina Revista Científica Multidisciplinar, 8(3), 3654-3671. DOI: https://doi.org/10.37811/cl_rcm.v8i3.11580

Meza Aranguren, V. J. (2024). ATFP. Aduana, tributos, finanzas y propiedad intelectual. Perspectivas sobre sus delitos. Corporación ATFP.

Meza Aranguren, V. J. (2024). El contrabando, defraudación fiscal y legitimación de capitales en la República Bolivariana de Venezuela. La Flechera, 1(14), 43-62. https://www.hormiguero.com.ve/download/revista-arbitrada-la-flechera-i-2024/

Naciones Unidas. (2025). Carta de las Naciones Unidas. https://www.un.org/es/about-us/un-charter/full-text

Pavlidis, G. (2020). El grupo de acción financiera (GAFI) treinta años después: el futuro de la lucha internacional contra el blanqueo de capitales y la financiación del terrorismo. Revista Estudios Jurídicos. Segunda Época, (20), 434-447. https://doi.org/10.17561/rej.n20.a18

Pérez Medina, D. (2020). Blockchain, criptomonedas y los fenómenos delictivos: entre el crimen y el desarrollo. Boletín criminológico, 26(197), 2-24. https://dialnet.unirioja.es/servlet/articulo?codigo=7701822

Piernas López, J. (2024). Las medidas de autotutela frente a amenazas cibernéticas en derecho internacional. Especial referencia a la posible adopción de contramedidas colectivas. Cuadernos de Derecho Transnacional, 16(1), 10-35. https://doi.org/10.20318/cdt.2024.8412

Pocar, F. (2004). New challenges for international rules against cyber-crime. European Journal on Criminal Policy and Research, 10(1), 27-37. https://doi.org/10.1023/B:CRIM.0000037565.32355.10

Pons, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO Revista Latinoamericana de Estudios de Seguridad, (20), 80-93. https://doi.org/10.17141/urvio.20.2017.2563

Rada, K. (2024). Herramientas de análisis forense digital orientadas a infraestructuras ti como medio de investigación en delitos informáticos. [Monografía]. Repositorio Institucional UNAD. https://repository.unad.edu.co/handle/10596/48990

Reedy, P. (2020). Interpol review of digital evidence 2016-2019. Forensic Science International: Synergy, 2, 489-520. https://doi.org/10.1016/j.fsisyn.2020.01.015

Resta, D. (2019). El principio nullum crimen, nulla poena sine lege en el derecho penal internacional. En particular en el Estatuto de la Corte Penal Internacional [tesis doctoral]. Universidad de Granada. https://digibug.ugr.es/handle/10481/54975

Ríos García, J. (2021). Ciberoperaciones realizadas por actores no estatales desde el territorio de un estado. La responsabilidad internacional de los Estados y el principio de diligencia debida [tesis de grado]. Comillas. Universidad Pontificia. https://repositorio.comillas.edu/

Rodríguez, G. S. (2016). Ciberseguridad realidad y tendencias en Venezuela. Cuestiones Jurídicas, 10(1),13-39. https://www.redalyc.org/journal/1275/127550463012/html/

Rodríguez, J. A., Oduber, J., y Mora, E. (2017). Routine activities and cyber-victimization in Venezuela. URVIO Revista Latinoamericana de Estudios de Seguridad, (20), 63-79. http://dx.doi.org/10.17141/urvio.20.2017.2583

Suganya Arawazhi, M. (2020). Understanding cyber crime and cyber laundering: threat and solution. International Journal of Research and Development, 5(1), 34-38. https://doi.org/10.36713/epra3902

Takei, Y. y Shudo, K. (2024). FATF Travel Rule's Technical Challenges and Solution Taxonomy. IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Dublin, Ireland, (pp. 784-799). https://r4d.mercari.com/fatf.pdf

Torres, D. (2018). Cyber security and cyber defense for Venezuela: an approach from the Soft Systems Methodology. Complex & Intelligent Systems, 4(3), 213-226. https://doi.org/10.1007/s40747-018-0068-x

Troya Aldaz, P. F., Vargas Almachi, M. A., Barrera Espín, C. J. y Barrera Espín, A. R. (2024). Criminología relacionada con los delitos cibernéticos y la falta de punibilidad de conductas. Ciencia Latina. Revista Científica Multidisciplinar, 8(6), 241-258. https://doi.org/10.37811/cl_rcm.v8i6.14605

Varela, L. (2024). Recuperación de activos como bastión contra la corrupción. UNIR. La Universidad en Internet. https://www.unir.net/revista/derecho/recuperacion-activos-bastion-contra-corrupcion/

Verde, G. (2025). Bit e Giustizia: Il Percorso della Prova Digitale nelle Attività di Digital Forensics, una review. i-lex. Rivista di Scienze Giuridiche, Scienze Cognitive e Intelligenza Artificiale, 18(1), 49-69. https://i-lex.unibo.it/article/view/21507

Wu, T., Breitinger, F. y O'Shaughnessy, S. (2020). Digital forensic tools: Recent advances and enhancing the status quo. Forensic Science International: Digital Investigation, 34, 1-17. https://doi.org/10.1016/j.fsidi.2020.300999