

El Iter Criminis Digital: Reconfiguración Dogmática y Desafíos Probatorios en el Derecho Penal Peruano

Juan Eduardo Valdera Olivos¹

¹Universidad César Vallejo (UCV), Chiclayo, Perú

jvalderao@ucvvirtual.edu.pe | <https://orcid.org/0009-0001-6317-1654>

Correspondencia: jvalderao@ucvvirtual.edu.pe

Resumen: El artículo examina cómo la transformación digital ha reconfigurado la comprensión tradicional del *iter criminis* en el derecho penal peruano, evidenciando que las categorías clásicas (fase interna, actos preparatorios, inicio de ejecución y consumación) resultan insuficientes frente a la rapidez, automatización y deslocalización propias del entorno informático. El estudio se desarrolló desde un enfoque cualitativo, mediante un diseño no experimental, transversal y documental, aplicando análisis de contenido a fuentes normativas y doctrinales, complementado con la sistematización analógica de siete resoluciones de la Corte Suprema del Perú sobre las categorías generales del *iter criminis*, ante la ausencia verificada de jurisprudencia suprema específica sobre cibercrimes, con el objetivo de reconstruir el *iter criminis* en los delitos informáticos de la Ley N.º 30096. Se analizó la incidencia de la norma en la redefinición del riesgo penalmente relevante y en el adelantamiento de punibilidad de actos preparatorios digitales, como la posesión de *malware*. Los resultados evidenciaron que la jurisprudencia suprema disponible sobre las categorías del *iter criminis* se concentra mayoritariamente en aspectos probatorios y procesales, revelando desafíos derivados de la volatilidad de la evidencia digital, la preservación de metadatos, la cadena de custodia digital y la necesidad de pericias informáticas especializadas. El estudio sostiene que la cibercriminalidad, por su naturaleza transnacional, exige fortalecer la cooperación internacional y modernizar las capacidades institucionales del sistema de justicia. Finalmente, se concluye que resulta necesaria una reinterpretación funcional del *iter criminis* digital que permita una persecución penal eficaz sin afectar los límites constitucionales del derecho penal de acto.

Palabras clave: iter criminis; cibercriminalidad peruana; evidencia digital; cadena de custodia; fraude informático.

Código de clasificación UNESCO: 5605.05 - Derecho penal.

Clasificación OCDE-FOS: 5.5 - Derecho.

The Digital Iter Criminis: Dogmatic Reconfiguration and Evidentiary Challenges in Peruvian Criminal Law

Abstract: This article examines how digital transformation has reconfigured the traditional understanding of the *iter criminis* in Peruvian criminal law, showing that the classical categories (internal phase, preparatory acts, commencement of execution, and consummation) are insufficient given the speed, automation, and delocalization characteristic of the digital environment. We conducted the study using a qualitative approach, through a non-experimental, cross-sectional, and documentary design, applying content analysis to normative and doctrinal sources, complemented by the analogical systematization of seven rulings of the Supreme Court of Peru on the general categories of the *iter criminis*, given the verified absence of specific Supreme Court case law on cybercrimes, with the aim of reconstructing the *iter criminis* in the computer-related offenses of Law No. 30096. We analyzed the impact of the statute on the redefinition of criminally relevant risk and on the advancement of the threshold of criminal liability for digital preparatory acts, such as the possession of malware. The findings showed that the available Supreme Court case law on the categories of the *iter criminis* focuses mainly on evidentiary and procedural aspects, revealing challenges arising from the volatility of digital evidence, the preservation of metadata, the digital chain of custody, and the need for specialized computer forensic expertise. The study argues that cybercrime, given its transnational nature, requires strengthening international cooperation and modernizing the institutional capacities of the justice system. Finally, a functional reinterpretation of the digital *iter criminis* is needed to allow effective criminal prosecution without undermining the constitutional limits of act-based criminal law.

Keywords: iter criminis; peruvian cybercrime; digital evidence; chain of custody; computer-related fraud.

UNESCO Classification Code: 5605.05 - Criminal law.

OECD-FOS Classification: 5.5 - Law.

O Iter Criminis Digital: Reconfiguração Dogmática e Desafios Probatórios no Direito Penal Peruano

Resumo: O artigo examina como a transformação digital reconfigurou a compreensão tradicional do *iter criminis* no direito penal peruano, evidenciando que as categorias clássicas (fase interna, atos preparatórios, início de execução e consumação) mostram-se insuficientes diante da rapidez, automação e deslocalização próprias do ambiente informático. O estudo foi desenvolvido a partir de uma abordagem qualitativa, por meio de um delineamento não experimental, transversal e documental, aplicando análise de conteúdo a fontes normativas e doutrinárias, complementada pela sistematização analógica de sete decisões da Corte Suprema do Peru sobre as categorias gerais do *iter criminis*, diante da ausência verificada de jurisprudência da Corte Suprema especificamente sobre crimes cibernéticos, com o objetivo de reconstruir o *iter criminis* nos crimes informáticos previstos na Lei n.º 30096. Analisou-se a incidência da norma na redefinição do risco penalmente relevante e na antecipação da punibilidade de atos preparatórios digitais, como a posse de *malware*. Os resultados evidenciaram que a jurisprudência da Corte Suprema disponível sobre as categorias do *iter criminis* concentra-se majoritariamente em aspectos probatórios e processuais, revelando desafios decorrentes da volatilidade da evidência digital, da preservação de metadados, da cadeia de custódia digital e da necessidade de perícias informáticas especializadas. O estudo sustenta que a cibercriminalidade, em razão de sua natureza transnacional, exige o fortalecimento da cooperação internacional e a modernização das capacidades institucionais do sistema de justiça. Por fim, conclui-se que é necessária uma reinterpretção funcional do *iter criminis* digital que permita uma persecução penal eficaz sem afetar os limites constitucionais do direito penal do fato.

Palavras-chave: iter criminis; cibercriminalidade peruana; evidência digital; cadeia de custódia; fraude informática.

Código de Classificação UNESCO: 5605.05 - Direito penal.

Classificação OCDE-FOS: 5.5 - Direito.

Cómo citar este artículo:

Valdera, J. E. (2026). El Iter Criminis Digital: Reconfiguración Dogmática y Desafíos Probatorios en el Derecho Penal Peruano. *Revista Científica*, 11(Ed. Esp. 3), 75–94. <https://doi.org/10.29394/Scientific.issn.2542-2987.2026.11.e3.5.75-94>

Fecha de Recepción:
14-11-2025

Fecha de Aceptación:
04-02-2026

Fecha de Publicación:
05-05-2026

1. Introducción

La irrupción del ciberespacio ha transformado de manera radical las formas en que se manifiesta la criminalidad contemporánea, planteando desafíos inéditos a categorías dogmáticas que, como el *iter criminis*, fueron concebidas para un derecho penal construido sobre conductas físicamente verificables. El presente artículo aborda esta problemática desde la perspectiva del derecho penal peruano, examinando cómo la automatización, el anonimato y la deslocalización del entorno digital reconfiguran la comprensión tradicional de las fases del delito. A continuación, se exponen el problema que orienta la investigación, su justificación y los objetivos que guían el análisis.

1.1. El Problema: El Derecho Penal ante el Desafío Digital

Tradicionalmente, la configuración delictiva en el derecho penal peruano se ha construido sobre la base de conductas físicamente apreciables: el forzamiento de una cerradura, la entrega de un documento falsificado o la realización de una acción exterior que deja una huella material verificable. Estas manifestaciones permitieron que categorías centrales, como el *iter criminis*, se diseñaran para describir con precisión el tránsito desde la ideación hasta la ejecución del hecho punible dentro de un marco espacio-temporal estable. Sin embargo, la irrupción del ciberespacio ha alterado profundamente este paradigma. El entorno digital, inmaterial, global y automatizado, ha generado nuevas modalidades de agresión penal caracterizadas por la deslocalización, la rapidez operativa, el anonimato tecnológico y la posibilidad de automatizar las acciones delictivas. Como advierten Zhou et al. (2024), estas transformaciones han desdibujado la frontera entre actos previos y actos ejecutivos, dificultando la identificación del riesgo penalmente relevante.

Frente a ello, la criminalidad informática comprime drásticamente las etapas del proceso delictivo y reduce la distancia funcional entre la preparación y la ejecución,

lo que genera tensiones interpretativas y riesgos de sobreextensión punitiva. A este problema se suma un segundo: la legitimidad constitucional del adelantamiento de punibilidad en actos preparatorios digitales, como la posesión de *malware*, que, bajo la teoría tradicional, carecerían de relevancia penal.

El presente trabajo se justifica en la necesidad de ofrecer una relectura dogmática sistemática del *iter criminis* digital, capaz de armonizar los principios del derecho penal de acto con las particularidades del riesgo automatizado propio del ciberespacio. Desde un enfoque dogmático-jurídico, se analizan la legislación peruana, la doctrina contemporánea y los criterios jurisprudenciales aplicables, con el propósito de delimitar con precisión cuándo una conducta informática trasciende la mera preparación para convertirse en acto ejecutivo.

El artículo se organiza de la siguiente manera: la Introducción expone el problema, las bases dogmáticas del *iter criminis* y las características del entorno digital regulado por la Ley N.º 30096; la Metodología describe el diseño documental y el corpus de resoluciones analizadas; los Resultados presentan la sistematización de la jurisprudencia suprema y la reconstrucción de las fases del delito en cinco figuras de dicha ley; y la Discusión contrasta estos hallazgos con la literatura, con énfasis en los desafíos probatorios y procesales.

1.2. Justificación e Importancia del Tema

La ciberdelincuencia no es una amenaza futura: hoy es ya una realidad cotidiana en el Perú. Hace apenas quince años, el acceso a equipos de cómputo y teléfonos celulares era limitado, y su uso se restringía a tareas básicas como la ofimática, la búsqueda de información o la mensajería de texto. La expansión de la conectividad digital ha transformado, sin embargo, los fundamentos de la educación, la ciencia, la tecnología, la comunicación, los negocios y las interrelaciones entre las personas y las autoridades. En la actualidad, ciudadanos pierden sus ahorros a causa de un correo electrónico fraudulento, mientras que empresas enteras ven secuestradas sus operaciones por un *ransomware*: el impacto es amplio y

creciente.

El Ministerio Público reporta, en ese sentido, un aumento constante en las denuncias por delitos informáticos. Este escenario exige que los operadores del derecho no solo conozcan la ley aplicable, como la Ley N.º 30096, sino que dominen la teoría del delito en este contexto particular. Un entendimiento preciso del *iter criminis* digital resulta crucial para determinar desde qué momento una conducta es penalmente relevante, cuál es el grado de desarrollo del delito y, en consecuencia, cómo debe graduarse la sanción de manera justa y proporcional, dentro de la garantía de un debido proceso constitucional. Esta exigencia es aún más estricta si se considera que la norma fundamental determina, en su artículo 2, numeral 24, literal d, que el derecho penal es de acto; en consecuencia, no podría sancionarse a quien no ha exteriorizado ni plasmado en el entorno digital una conducta objetivamente verificable que trasgreda un bien jurídico.

1.3. Bases Dogmáticas del *Iter Criminis* en el Ordenamiento Peruano

Para comprender la complejidad del delito en el ciberespacio, resulta necesario asentar primero las bases de cómo el derecho penal peruano ha entendido tradicionalmente el camino del crimen. La dogmática penal clásica ha distinguido, desde una perspectiva funcionalista, entre una fase interna, correspondiente al pensamiento, y una fase externa, correspondiente a la acción misma del delito. En esa línea, puede afirmarse que el camino del delito es, en esencia, la biografía de un ilícito, y que este recorrido se divide en dos grandes etapas con consecuencias jurídicas radicalmente distintas.

1.3.1. La Fase Interna: de la Idea a la Resolución (Impunidad como Regla General)

La génesis del delito se ubica en la esfera estrictamente psíquica del individuo. Esta fase inicial tiene naturaleza interna y, por ello, permanece fuera del alcance del derecho penal. La doctrina contemporánea mantiene de manera unánime que en esta etapa rige

plenamente el principio *cogitationis poenam nemo patitur*, fundamento del derecho penal de acto. Cabe enfatizar que el derecho penal solo puede intervenir frente a comportamientos exteriorizados que generen un riesgo jurídicamente relevante, criterio que evita la incriminación del pensamiento.

En la misma línea, puede sostenerse que ninguna teoría del delito moderna admite la sanción de pensamientos o intenciones, pues ello quebrantaría el núcleo del Estado constitucional. A esta postura se suma la advertencia de que la punición del pensamiento constituiría una deriva hacia un derecho penal de autor incompatible con la libertad mental garantizada por la Constitución.

Esta fase interna comprende tres momentos psicológicos. El primero es la ideación, entendida como el surgimiento de la idea delictiva; se trata del punto germinal del plan criminal, aún carente de toda relevancia jurídico-penal por no exteriorizar ningún riesgo. El segundo momento es la deliberación, en el que el sujeto pondera ventajas y riesgos; esta etapa representa un espacio de autonomía personal protegido por el derecho penal, incluso cuando las valoraciones internas sean moralmente reprochables. El tercer momento corresponde a la resolución, es decir, la decisión firme de actuar; incluso en este estadio, donde la voluntad delictiva se ha formado totalmente, el derecho penal sigue siendo ajeno porque no existe una conducta objetivable: la decisión interna, aun cuando sea definitiva, no compromete ningún bien jurídico.

La dimensión constitucional peruana refuerza esta conclusión. El artículo 2, numeral 24, literal d, de la Constitución consagra expresamente el derecho penal de acto, proscribiendo cualquier forma de persecución basada en el pensamiento. Esta garantía constituye un límite infranqueable: solo la exteriorización de la voluntad a través de un comportamiento perceptible habilita la intervención del *ius puniendi*. A nivel jurisprudencial, la Corte Suprema peruana ha reafirmado esta posición, aunque no en un caso de ciberdelincuencia: en la Casación N.º 37-2018-Cusco (Sala Penal Transitoria, 20

de agosto de 2019), en un proceso por robo agravado, precisó que la ideación, en cuanto actividad puramente mental, queda fuera del alcance punitivo porque el pensamiento resulta inaccesible a cualquier forma de conocimiento externo, criterio trasladable por analogía a la ciberdelincuencia.

Desde la perspectiva del derecho penal digital, diversos autores actuales han resaltado que el anonimato y la rapidez de la tecnología no alteran este principio. Conforme señalan Zhou et al. (2024), incluso en materia de ciberdelincuencia la automatización tecnológica difumina las categorías tradicionales sin suprimir la exigencia de una manifestación objetiva mínima, como la manipulación de herramientas tecnológicas o la interacción con sistemas informáticos. En igual sentido, cabe sostener, conforme a la dogmática penal general, que la era digital no autoriza un adelantamiento de la punibilidad hasta el terreno mental.

En consecuencia, hasta este estadio el ordenamiento jurídico permanece deliberadamente indiferente, pues no se ha producido una conducta que pueda crear peligro concreto para un bien jurídico. La impunidad de la fase interna constituye, por tanto, una garantía esencial del Estado constitucional de derecho: solo con la exteriorización de la voluntad delictiva a través de cualquier acto objetivamente verificable se abre la posibilidad de intervención penal.

1.3.2. La Fase Externa: la Materialización del Plan Criminal

La fase externa se inicia cuando el sujeto deja atrás el plano mental y exterioriza una conducta perceptible, generando un riesgo real para el bien jurídico. En este momento, el derecho penal abandona su indiferencia y activa su función de protección, pues ya existe una manifestación concreta del plan criminal. La doctrina reciente sostiene que esta etapa debe evaluarse según el grado de riesgo creado, lo que permite distinguir entre actos preparatorios, inicio de ejecución y consumación. En esta línea, la fase externa marca el tránsito desde la libertad interna hacia un ámbito de

relevancia social que justifica la intervención del *ius puniendi*.

Esta distinción adquiere especial importancia en materia digital, donde la compresión entre preparación y ejecución, advertida en el planteamiento del problema, dificulta determinar cuándo una conducta comienza a ser penalmente relevante. A falta de pronunciamientos supremos específicos sobre delitos informáticos, resulta ilustrativo el criterio fijado en la Casación N.º 1711-2019- Amazonas (Sala Penal Permanente, 29 de abril de 2022), que, en un caso de banda criminal y robo agravado en grado de tentativa, precisó que la fase externa comprende dos momentos, los actos preparatorios y los actos de ejecución, y caracterizó estos últimos como aquellos comportamientos, activos u omisivos, mediante los cuales el agente va realizando el tipo penal que se le atribuye; criterio aplicable por analogía a la ciberdelincuencia, centrado en la creación de un riesgo concreto y no en la intención subjetiva del agente.

1.3.3. Los Actos Preparatorios: Concepto y Punición Excepcional

Los actos preparatorios comprenden conductas que buscan facilitar la ejecución futura del delito, pero que, por su ambigüedad, no constituyen todavía el inicio de la acción típica. En esta etapa, el riesgo para el bien jurídico es aún hipotético, pues, como explica Bein (1993), la mayoría de los actos previos a la ejecución son equívocos y compatibles con finalidades lícitas, lo que impide su sanción bajo el principio de mínima intervención penal. Por ello, el derecho penal peruano mantiene como regla general la impunidad de estos actos, dado que no revelan por sí solos una voluntad delictiva inequívoca.

No obstante, la política criminal contemporánea ha reconocido que ciertos actos preparatorios trascienden su naturaleza ambigua y adquieren una peligrosidad tal que justifica su tipificación autónoma. Estos supuestos se justifican cuando la conducta previa exhibe un “peligro cualificado” y evidencia un grado de concreción incompatible con la mera planificación

interna. Así ocurre con las figuras de conspiración, proposición delictiva, tenencia ilegal de armas o preparación para cometer terrorismo o tráfico ilícito de drogas.

En el plano jurisprudencial, no se conocen pronunciamientos de la Corte Suprema peruana que apliquen este estándar a los actos preparatorios digitales, aspecto que se examina en los Resultados. La doctrina penal sostiene, no obstante, de manera consistente que la punición excepcional de actos preparatorios exige que la conducta revele una orientación inequívoca hacia la afectación del bien jurídico, pues de lo contrario se vulneraría el derecho penal de acto, y que la criminalización anticipada solo resulta legítima cuando existe una peligrosidad objetiva verificable, y no meras sospechas subjetivas del intérprete.

En el contexto de la ciberdelincuencia, esta lógica adquiere una importancia singular. La velocidad de los ataques informáticos y la capacidad de daño masivo justifican que legislaciones modernas, incluida la peruana mediante la Ley N.º 30096, tipifiquen de manera autónoma conductas como la creación o posesión de *malware*, que en un delito común serían actos preparatorios impunes. Este adelantamiento de las barreras de punición constituye, por tanto, una herramienta necesaria frente al riesgo cualificado propio del entorno digital.

1.3.4. La Tentativa: Inicio de la Ejecución y su Regulación en el Código Penal

La tentativa constituye el momento decisivo en el *iter criminis*, pues marca el paso desde la preparación hacia la ejecución del delito. El artículo 16 del Código Penal peruano establece que hay tentativa cuando el agente, habiendo resuelto cometer un delito, da inicio a su ejecución sin llegar a consumarlo. Para que este estadio se configure, la acción debe crear un riesgo inminente para el bien jurídico, lo que exige una proximidad objetiva y no meras conductas preparatorias, conforme a la doctrina penal general sobre la tentativa.

En la dogmática reciente, la tentativa se divide en inacabada, cuando el sujeto inicia la ejecución, pero no realiza todos los actos necesarios, y acabada, cuando ejecuta completamente el plan delictivo, pero la consumación no se produce por intervención externa o circunstancias no previstas. Esta clasificación permite graduar la punibilidad según la intensidad del riesgo creado.

Uno de los debates más complejos es la delimitación entre el último acto preparatorio y el primer acto ejecutivo. La Casación N.º 1711-2019-Amazonas (Sala Penal Permanente, 29 de abril de 2022) abordó reiteradamente esta frontera al desarrollar las distintas teorías sobre el inicio de ejecución, precisando que, conforme a la teoría objetivo-material, la acción comienza en el momento en que el bien jurídico tutelado ya se ve expuesto a un peligro directo e inmediato, y que la teoría mixta integra criterios de orden subjetivo y objetivo, de manera que, para determinar cuándo comienza la ejecución, debe tomarse en consideración el plan del autor, pero valorado desde un prisma objetivo de peligro para el bien jurídico. Aunque este pronunciamiento corresponde a un caso de robo agravado en grado de tentativa, sus criterios resultan trasladables por analogía a la determinación del inicio de ejecución en delitos informáticos.

La doctrina más reciente subraya que estos criterios deben interpretarse también a la luz de los delitos informáticos. En los ciberdelitos, la tentativa implica identificar el momento exacto en que una acción digital, como desplegar un *script* malicioso, pasa de ser preparación técnica a ejecución directa del ilícito. En suma, la tentativa representa el umbral crítico en que la conducta del agente ya amenaza de manera inmediata el bien jurídico, justificando plenamente la reacción penal.

1.3.5. La Consumación y el Agotamiento del Delito

La consumación representa el momento en que todos los elementos del tipo penal se materializan, consolidándose la lesión o puesta en peligro del bien jurídico. Cabe precisar que la consumación no depende

del resultado subjetivo que el agente espera lograr, sino del cumplimiento objetivo de la descripción típica. Así, en un robo la consumación se configura con el apoderamiento del bien, y en un homicidio, con la muerte de la víctima, sin que sea necesario que el autor alcance un beneficio adicional.

Debe distinguirse esta etapa del agotamiento, concepto que alude a la obtención de la finalidad última perseguida por el autor. Aunque forma parte del desarrollo fáctico del delito, el agotamiento generalmente carece de relevancia para la tipicidad, pero puede incidir en la determinación de la pena al evidenciar un mayor grado de realización del plan delictivo. En delitos como la extorsión, por ejemplo, la consumación ocurre con la amenaza que determina la disposición patrimonial de la víctima, mientras que el cobro efectivo del dinero constituye el agotamiento del delito.

La jurisprudencia peruana reafirma esta distinción, aunque en el marco de delitos patrimoniales clásicos. En el Recurso de Nulidad N.º 2181-2019-Lima (f. j. 8), la Corte Suprema estableció que la estafa queda consumada una vez que concluyen las maniobras engañosas desplegadas por el agente, criterio que ilustra el principio general según el cual la consumación se identifica atendiendo a la realización objetiva del tipo penal, con independencia del provecho ulterior que el agente pretenda obtener, lo que corresponde propiamente al agotamiento del delito.

Ante la ausencia de jurisprudencia suprema peruana publicada que aplique específicamente este criterio a los ciberdelitos, dicho estándar se traslada por analogía al ámbito digital. En suma, la consumación implica la realización plena del tipo penal y marca el término del *iter criminis* relevante para la imputación típica; el agotamiento, en cambio, corresponde a una fase posterior, carente de efectos en la tipicidad, pero que puede adquirir relevancia para valorar el reproche penal o la gravedad del hecho.

1.4. El Ciberespacio como Nuevo Paradigma Criminológico

Establecidas las bases tradicionales, corresponde examinar el factor que las altera: el ciberespacio. Este no constituye simplemente un nuevo escenario para cometer viejos delitos, sino un entorno con características propias que obligan a reevaluar los conceptos dogmáticos clásicos. Los entornos digitales, como las redes sociales, el comercio electrónico, el almacenamiento de datos en la nube, la banca en línea y los servicios digitales gubernamentales, se encuentran hoy regulados y protegidos de manera desigual frente a los posibles ataques de los ciberdelinquentes, quienes actúan de manera anónima y clandestina detrás de un dispositivo electrónico y un medio telemático para exteriorizar su conducta delictiva.

Estos ataques afectan bienes jurídicos que, en muchos casos, aún no se encuentran reconocidos de manera categórica en el ordenamiento peruano, como el derecho a la protección de datos personales, el derecho a una identidad digital, el derecho a contar con determinadas cuentas de IP o el derecho a disponer de tecnologías adecuadas para el desarrollo sostenible de una sociedad digital, entre las que destaca la traducción de direcciones de red (NAT), tecnología que permite a múltiples dispositivos de una red privada compartir una misma dirección IP pública.

1.4.1. Características del Entorno Digital: Anonimato, Velocidad y Deslocalización

El entorno digital permite niveles elevados de anonimato mediante herramientas como redes privadas virtuales (VPN), servidores *proxy* o la red Tor, lo que dificulta la identificación del autor y reduce la inhibición delictiva. Para Zhou et al. (2024), la difuminación de categorías propia del entorno digital se refleja también en el anonimato tecnológico, que favorece que el agente oculte su identidad y ubicación y exige capacidades técnicas avanzadas para la atribución penal. A esta ocultación se suman la velocidad y la automatización propias del entorno: los ataques informáticos pueden

ejecutarse en milisegundos y replicarse automáticamente a través de *bots*, *malware* o *scripts* autónomos. Desde una perspectiva técnica, Das et al. (2020) destacan que esta dinámica comprime el *iter criminis* al reducir a una sola acción la distancia entre la deliberación y la ejecución; ello plantea, desde la dogmática penal, el desafío de determinar cuándo empieza realmente la tentativa en el ámbito digital.

A ello se añaden la deslocalización y la transnacionalidad: las conductas delictivas pueden originarse en un país, ejecutarse desde servidores ubicados en otro y afectar a víctimas en múltiples jurisdicciones. En este sentido, Casino et al. (2022) resaltan que esta deslocalización diluye los criterios clásicos de territorialidad penal y exige una coordinación internacional más robusta para la persecución eficaz de ciberdelitos. En este contexto, el Convenio de Budapest sobre Ciberdelincuencia, ratificado por el Perú, se convierte en el principal marco de cooperación para la preservación y el intercambio de evidencia digital a nivel internacional.

1.4.2. La Ley N.º 30096 y su Marco de Actuación en el Perú

La Ley N.º 30096 constituye la respuesta normativa central del Estado peruano frente a los desafíos que plantea el entorno digital. Promulgada en 2013 y posteriormente complementada por diversas reformas, esta ley no solo introdujo tipos penales específicos para enfrentar la criminalidad informática, sino que también modificó disposiciones del Código Penal y del Código Procesal Penal con el fin de adecuar instituciones tradicionales a las particularidades del ciberespacio.

Su estructura se fundamenta en la protección de tres dimensiones esenciales del ecosistema informático: la confidencialidad, la integridad y la disponibilidad de los datos y sistemas digitales, modelo conocido como “CID”. Esta tríada permite articular un sistema de tutela penal que abarca tanto los ataques directos a la infraestructura tecnológica como la instrumentalización digital de delitos

clásicos, entre ellos el fraude informático, la suplantación de identidad o el acceso ilícito.

La Ley N.º 30096 incorpora, además, figuras de adelantamiento de punibilidad, como la producción o posesión de herramientas informáticas maliciosas (art. 10), las cuales, en la estructura tradicional del *iter criminis*, serían simples actos preparatorios. La inclusión de estos delitos autónomos evidencia un modelo de prevención reforzada frente al alto potencial lesivo del *malware* y la facilidad de su despliegue masivo en cuestión de segundos, propio de la política criminal frente a la ciberdelincuencia digital.

Desde el plano interpretativo, esta ley opera como el marco de referencia para reconstruir el *iter criminis* digital en el Perú. La delimitación entre actos preparatorios, tentativa y consumación debe analizarse a la luz de los comportamientos técnicos previstos en los artículos 2 al 11, lo que obliga a precisar, para cada tipo penal, qué comportamiento técnico constituye un “inicio de ejecución” en un ataque digital. El marco normativo se complementa con el Convenio de Budapest, cuyo papel en la cooperación internacional ya se ha señalado. En conjunto, la Ley N.º 30096 constituye el núcleo del derecho penal informático peruano y orienta la reconstrucción dogmática del *iter criminis* en entornos digitales.

1.5. Pregunta y Objetivos de la Investigación

En atención al problema expuesto, la investigación se orienta por la siguiente pregunta: ¿siguen siendo suficientes las categorías clásicas del *iter criminis* para delimitar los actos preparatorios, el inicio de ejecución y la consumación en los ciberdelitos regulados por la Ley N.º 30096, o es necesaria una reinterpretación dogmática adaptada a las particularidades del entorno digital? En correspondencia con ella, el objetivo general consiste en analizar el *iter criminis* en los delitos informáticos de la Ley N.º 30096, a partir de los criterios de la Corte Suprema del Perú aplicables por analogía, para delimitar sus fases y los desafíos probatorios que plantea su acreditación en sede penal.

De este objetivo se desprenden tres objetivos específicos: primero, sistematizar los criterios de la Corte Suprema sobre las categorías generales del *iter criminis* y verificar si existe su aplicación específica a los ciberdelitos; segundo, reconstruir las fases de actos preparatorios, tentativa y consumación en cinco tipos penales de la Ley N.º 30096; y tercero, identificar los principales desafíos sustantivos, procesales y probatorios para acreditar dichas fases en investigaciones de ciberdelitos.

2. Metodología

La investigación adoptó un enfoque cualitativo, orientado a comprender e interpretar de manera sistemática un corpus documental normativo, doctrinal y jurisprudencial propio de la dogmática penal; de acuerdo con Hernández-Sampieri y Mendoza (2018), este enfoque resulta pertinente cuando se busca examinar un fenómeno a partir del sentido que le atribuyen las fuentes analizadas. El método empleado fue el análisis de contenido cualitativo, aplicado a un estudio de casos jurisprudenciales, procedimiento que, tal como lo describen Creswell y Creswell (2018), consiste en la codificación y agrupación temática de la información documental para identificar patrones de significado.

El diseño correspondió a una investigación no experimental, transversal y documental, puesto que las fuentes se examinaron tal como fueron producidas, sin manipulación de variables y en un único corte temporal (Cohen et al., 2018; Hernández-Sampieri & Mendoza, 2018). Por su finalidad, la investigación fue de tipo aplicado, en la medida en que se propuso ofrecer criterios funcionales de utilidad directa para fiscales, jueces y peritos en la acreditación del *iter criminis* digital.

La búsqueda documental se orientó, en primer término, a identificar resoluciones de la Corte Suprema de Justicia del Perú que aplicaran específicamente las categorías del *iter criminis* a los delitos informáticos de la Ley N.º 30096, mediante los términos “*iter criminis*”, “ciberdelitos”, “Ley N.º 30096”, “evidencia digital”, “cadena de custodia” y “pericia informática forense” en el

sistema de jurisprudencia del Poder Judicial del Perú y en repositorios especializados (LP Derecho, Gaceta Jurídica, vLex Perú). Esta búsqueda arrojó un hallazgo relevante: la Corte Suprema peruana no ha publicado, hasta la fecha, jurisprudencia que aplique de manera específica dichas categorías a los tipos penales de la Ley N.º 30096. Ante este vacío, la muestra se reorientó, mediante un muestreo no probabilístico intencional, hacia siete resoluciones de la Corte Suprema, emitidas entre 2019 y 2024, que desarrollan los criterios generales de la fase interna, la fase externa, la tentativa, la consumación y la valoración de la evidencia digital en otras figuras penales (robo agravado, estafa, peculado), seleccionadas por su pertinencia para una reconstrucción del *iter criminis* digital por analogía.

Como instrumento de recolección y análisis de datos se empleó una ficha de análisis documental elaborada *ad hoc*, que registró, para cada resolución, el número de expediente, la figura penal de origen, el año de emisión y el criterio jurídico establecido por la Corte Suprema. Sobre esta base, se aplicó un proceso de codificación temática, en el que cada resolución fue clasificada según la categoría del *iter criminis* a la que resultaba pertinente por analogía: fase interna, fase externa, tentativa, consumación, o aspectos probatorios y procesales.

El procedimiento consistió en la lectura íntegra de cada resolución, la extracción de la *ratio decidendi* o criterio jurídico relevante, su codificación conforme a las categorías señaladas y, finalmente, la sistematización de los resultados en una tabla comparativa que permitiera visibilizar tanto los criterios dogmáticos disponibles como el vacío jurisprudencial identificado respecto de su aplicación específica a los ciberdelitos.

El método de análisis empleado fue, además, descriptivo, sistemático, comparado y crítico frente a las fuentes normativas y doctrinales. En primer lugar, se describieron las categorías tradicionales del *iter criminis*; luego, se sistematizaron las características técnicas del ciberespacio que inciden en la determinación de las fases del delito. En tercer lugar, se realizó un análisis

comparado entre el modelo clásico y el modelo digital para identificar rupturas, reconfiguraciones y nuevas exigencias dogmáticas, contrastando dicho análisis con los criterios efectivamente adoptados por la Corte Suprema en el corpus jurisprudencial estudiado. Finalmente, se desarrolló un examen crítico orientado a valorar la suficiencia de las categorías tradicionales frente a la dinámica delictiva digital y a proponer criterios interpretativos que permitieran delimitar adecuadamente la relevancia penal de las conductas informáticas.

Se emplearon también fuentes primarias normativas, como el Código Penal peruano, la Ley N.º 30096 y el Convenio de Budapest, y fuentes secundarias de doctrina penal general y dogmática digital, nacional y extranjera. Para contrastar estos planteamientos con evidencia académica verificable, se revisaron trabajos sobre evidencia digital, cadena de custodia, jurisdicción transfronteriza, investigación forense y ciberdelincuencia (Aksamitowska, 2021; Al-Faraji, 2025; Alhawawsheh et al., 2025; Alluqmani et al., 2025; Bein, 1993; Bigos, 2005; Caputo et al., 2014; Casino et al., 2022; Cross & Blackshaw, 2015; Das et al., 2020; Dragojlović, 2023; Garfinkel, 2009; Greene et al., 2018; Hutchings et al., 2016; Ingemarsson et al., 2025; Irawan et al., 2025; Iuga et al., 2016; Jagatic et al., 2007; Kumaraguru et al., 2007, 2010; Leukfeldt et al., 2017; Lewulis, 2022; Logos et al., 2023; Novak, 2022; Ofori & Akoto, 2020; Sheng et al., 2010; Sousa-Silva, 2024; Sutter et al., 2022; Wang, 2025; Zhou et al., 2024).

Entre estos estudios, Jagatic et al. (2007) e Iuga et al. (2016) documentan los factores psicológicos que incrementan la susceptibilidad al *phishing*, mientras que Kumaraguru et al. (2007, 2010) y Sutter et al. (2022) evalúan la efectividad limitada de la capacitación *anti-phishing*; por su parte, Novak (2022) y Bigos (2005) aportan elementos sobre la admisibilidad de la evidencia digital y la jurisdicción transfronteriza, retomados en la Discusión. El alcance de la investigación combinó así la reconstrucción conceptual y normativa propia de la dogmática penal con la sistematización de los criterios jurisprudenciales disponibles, aplicados por analogía a la

ciberdelincuencia.

3. Resultados

En esta sección se presentan los hallazgos del análisis documental, organizados en dos bloques. Primero, se exponen los resultados de la búsqueda y sistematización de la jurisprudencia de la Corte Suprema sobre las categorías generales del *iter criminis*, sintetizados en la tabla 1. Segundo, se reconstruyen, a partir de esos criterios y del marco normativo, las fases del *iter criminis* en cinco figuras penales de la Ley N.º 30096, cuya comparación con el modelo clásico se resume en la tabla 2.

3.1. El Vacío Jurisprudencial Específico y la Aplicación Analógica de Criterios Generales del *Iter Criminis*

La búsqueda sistemática descrita en la Metodología arrojó un primer hallazgo empírico: la Corte Suprema de Justicia del Perú no ha publicado, hasta la fecha, resoluciones que apliquen de manera específica las categorías del *iter criminis* a los tipos penales de la Ley N.º 30096. En consecuencia, el corpus quedó integrado por las siete resoluciones de alcance general seleccionadas conforme a los criterios allí expuestos.

Tabla 1. Jurisprudencia General Aplicable por Analogía a las Categorías del *Iter Criminis* Digital (N = 7).

N.º	Resolución	Año	Materia de Origen	Categoría (por analogía)	Criterio Jurídico Central
1	Casación N.º 37-2018-Cusco	2019	Robo agravado	Fase interna	La ideación, como proceso cognitivo, no es punible por la imposibilidad de conocer el pensamiento del agente. La fase externa comprende actos preparatorios y actos de ejecución; el inicio de ejecución exige una puesta en peligro directa e inmediata del bien jurídico. La estafa se consuma desde el momento en que cesaron las maniobras fraudulentas. El código <i>hash</i> constituye el mecanismo idóneo para garantizar la autenticidad de la evidencia digital. Las irregularidades en la cadena de custodia no vulneran por sí mismas un derecho fundamental, salvo que alcancen la gravedad de una ruptura.
2	Casación N.º 1711-2019-Amazonas	2022	Banda criminal / robo agravado (tentativa)	Fase externa y tentativa	La ruptura de la cadena de custodia es un acto irregular que no determina
3	Recurso de Nulidad N.º 2181-2019-Lima	2019	Estafa	Consumación	
4	Apelación N.º 77-2024	2024	Valoración de evidencia digital (audio/video)	Aspectos probatorios	
5	Casación N.º 1669-2021-Loreto	2023	Cadena de custodia	Aspectos probatorios	
6	Recurso de Nulidad N.º 1714-2023-Lima Sur	2024	Cadena de custodia	Aspectos probatorios	

N.º	Resolución	Año	Materia de Origen	Categoría (por analogía)	Criterio Jurídico Central
7	Recurso de Nulidad N.º 7-2021-Puno	2021	Peculado	Aspectos probatorios	automáticamente la nulidad o inutilización del medio probatorio. La valoración deficiente de la pericia técnica, sin considerar su contexto integral, invalida la acreditación de los hechos imputados.

Nota. Fuente: Valdera (2025). Elaboración a partir del análisis de contenido cualitativo de siete resoluciones de la Corte Suprema de Justicia del Perú (2019-2024), seleccionadas conforme al procedimiento descrito en la Metodología. Ninguna versa específicamente sobre ciberdelitos.

La tabla 1 evidencia dos hallazgos complementarios. Por un lado, confirma un desarrollo jurisprudencial consolidado sobre las categorías clásicas del *iter criminis* en delitos tradicionales: la Casación N.º 37-2018-Cusco delimita la fase interna como el momento cognitivo no punible, la Casación N.º 1711-2019-Amazonas desarrolla, en un caso de robo agravado en tentativa, la fase externa y los criterios objetivo-material y mixto para el inicio de ejecución, y el Recurso de Nulidad N.º 2181-2019-Lima fija el criterio de consumación a partir del cese de las maniobras fraudulentas.

Por otro lado, revela que la mayor concentración de jurisprudencia disponible corresponde a los aspectos probatorios, con cuatro de las siete resoluciones: la Apelación N.º 77-2024 reconoce el *hash* como garantía de autenticidad de la evidencia digital, la Casación N.º 1669-2021-Loreto y el Recurso de Nulidad N.º 1714-2023-Lima Sur precisan que la ruptura de la cadena de custodia solo compromete la prueba cuando alcanza gravedad sustancial, y el Recurso de Nulidad N.º 7-2021-Puno establece que la valoración pericial deficiente invalida la acreditación de los hechos. No se identificó, finalmente, jurisprudencia suprema que desarrolle la categoría de actos preparatorios en clave digital, un vacío adicional.

3.2. Análisis del *Iter Criminis* en los Ciberdelitos de la Ley N.º 30096

A partir de los criterios sistematizados en la tabla 1 y del marco normativo descrito en la Introducción, se reconstruyeron las fases del *iter criminis* en cinco figuras

penales concretas de la Ley N.º 30096: el acceso ilícito, el ataque a la integridad de datos, la posesión de *software* malicioso, el fraude informático y la suplantación de identidad.

3.2.1. El Acceso Ilícito (Art. 2): Actos Preparatorios y Tentativa

El artículo 2 de la Ley N.º 30096 sanciona a quien, de forma intencional y sin autorización, ingresa total o parcialmente a un sistema informático. Para ilustrar sus fases, puede imaginarse a un joven *hacker* que pretende acceder a la base de datos de notas de su universidad.

En la fase interna se genera la idea, se ponderan los riesgos y beneficios, y el sujeto resuelve actuar. En los actos preparatorios impunes, el agente indaga sobre las posibles vulnerabilidades del sistema de la universidad, descargas manuales de *hacking* y estudia el lenguaje de programación del portal: son acciones aún ambiguas. Distinto es el caso de los actos preparatorios punibles como delito autónomo: si el *hacker* crea u obtiene un programa diseñado para explotar una vulnerabilidad conocida del sistema, su conducta podría encajar en el artículo 10 de la ley, por lo que podría ser sancionado incluso antes de lanzar el ataque.

La tentativa se configura cuando el agente ejecuta un *script* de fuerza bruta que prueba miles de contraseñas por segundo: aunque no ha logrado acceder, ya no está preparando, sino atacando directamente la barrera de seguridad. La consumación se produce cuando el sistema acepta una contraseña y concede el acceso, aunque sea por un instante: el delito de acceso ilícito ya se ha consumado, pues el bien jurídico “confidencialidad” ha sido vulnerado.

3.2.2. El Ataque a la Integridad de Datos (Art. 3): la Consumación en los Ataques de *Malware*

El artículo 3 de la Ley N.º 30096 sanciona a quien, de manera deliberada e ilegítima, inutiliza total o parcialmente, altera, daña o suprime datos informáticos. El ejemplo paradigmático es el ataque de *ransomware*.

En los actos preparatorios, un grupo de ciberdelincuentes programa un *ransomware* o lo

adquiere en la *dark web*. Posteriormente, envía un correo de *phishing* a los empleados de una empresa peruana con el *malware* oculto en un archivo adjunto. Dicho envío, en tanto contiene el medio idóneo para dañar los datos, constituye ya un acto ejecutivo que califica como tentativa. La consumación, por su parte, no se produce cuando el empleado hace clic en el archivo, sino en el instante en que el *malware* comienza a cifrar los archivos del sistema, haciéndolos inaccesibles para la empresa: en ese preciso momento se pierden la integridad y la disponibilidad de los datos, sin que sea necesario que los delincuentes exijan el rescate o que la empresa lo pague, pues eso correspondería ya al agotamiento del plan criminal.

3.2.3. El Abuso de Mecanismos y Dispositivos Informáticos (Art. 10): la Posesión de Software Malicioso como Adelantamiento de las Barreras de Punición

El legislador peruano, siguiendo una tendencia internacional, decidió criminalizar de forma autónoma ciertos actos que son netamente preparatorios para la comisión de otros ciberdelitos. El artículo 10 de la Ley N.º 30096, cuyo título oficial es "Abuso de mecanismos y dispositivos informáticos", sanciona la fabricación, diseño, desarrollo, venta, facilitación, distribución o importación de *software* malicioso (*malware*), contraseñas, códigos de acceso o dispositivos informáticos, con el propósito de cometer los delitos previstos en la ley.

Esta decisión político-criminal se fundamenta en la alta peligrosidad inherente a estas herramientas: un *malware* puede desplegarse a escala masiva en segundos, causando daños irreparables, de modo que esperar a que se inicie el ataque, es decir, a la tentativa, resultaría demasiado tardío. Por ello, se sanciona la simple tenencia finalista, en una clara manifestación de un acto preparatorio que, por excepción, es punible.

3.2.4. El Fraude Informático (Art. 8): del *Phishing* a la Consumación del Menoscabo Patrimonial

El artículo 8 de la Ley N.º 30096 sanciona al

agente que, mediante la alteración, manipulación o interferencia de datos o sistemas informáticos, obtiene para sí o para otro un beneficio ilícito en perjuicio de terceros. Dentro de estas modalidades, el *phishing* constituye una de las manifestaciones más frecuentes y sofisticadas, sustentado en la ingeniería social combinada con técnicas de clonación digital que permiten engañar a la víctima para obtener sus credenciales financieras o datos sensibles. En relación con esta modalidad, Cross y Blackshaw (2015) destacan las dificultades que enfrenta la respuesta policial frente al fraude en línea derivado de este tipo de ataques.

En la fase interna y los actos preparatorios, el sujeto idea el plan, selecciona la entidad bancaria objetivo y registra un dominio falsificado similar al oficial; luego clona la interfaz de la plataforma digital y diseña un mensaje fraudulento destinado a generar alarma. Como señalan Das et al. (2020), la preparación técnica del *phishing* puede ser extensa y sofisticada, aunque no implica todavía un ataque directo contra un bien jurídico. Por ello, desde la dogmática penal, estas conductas, orientadas al ilícito, siguen siendo equívocas y constituyen actos preparatorios.

La tentativa se configura cuando el agente inicia el despliegue del engaño mediante el envío masivo de correos electrónicos fraudulentos. En este punto, la conducta deja de ser equívoca, pues el "ardid informático" ya se encuentra en ejecución, conforme al criterio objetivo-material desarrollado por la Corte Suprema en la Casación N.º 1711-2019-Amazonas, según el cual el inicio de ejecución se configura cuando la conducta expone al bien jurídico tutelado a un peligro directo e inmediato, incluso sin lograr su resultado final.

La consumación ocurre cuando la víctima, inducida a error, ingresa a la página clonada y registra sus credenciales, permitiendo que el agente acceda a su cuenta bancaria y efectúe una transferencia no autorizada. La consumación del fraude digital se produce con el desplazamiento patrimonial automatizado, sin que sea necesario que el autor retire físicamente el dinero, en línea con el criterio general de la Corte Suprema peruana

según el cual la estafa alcanza su consumación al finalizar las maniobras fraudulentas (Recurso de Nulidad N.º 2181-2019-Lima, f. j. 8), aplicable por analogía a la manipulación informática. Bajo esta estructura, el fraude informático revela un *iter criminis* comprimido, en el que la ejecución digital acelera el tránsito desde la preparación hacia la consumación.

3.2.5. La Suplantación de Identidad (Art. 9): el Camino Delictivo desde la Creación del Perfil Falso

Este delito, previsto en el artículo 9 de la Ley N.º 30096, sanciona a quien, mediante las tecnologías de la información, sustituye la identidad de una persona física o jurídica para inducir a error y obtener un beneficio o causar un perjuicio.

El camino delictivo comienza con la creación deliberada de un perfil falso en una red social, usando el nombre y las fotografías de la víctima. Este acto ya puede considerarse el inicio de la ejecución, es decir, la tentativa, pues constituye la acción idónea y directa de “suplantar” en el entorno digital. El delito se consuma cuando el suplantador interactúa con terceros, por ejemplo, enviando mensajes a los amigos de la víctima para pedirles dinero, induciéndolos a error sobre su identidad, independientemente de si logra o no el perjuicio económico. En este tipo penal, por tanto, no existirían propiamente actos preparatorios autónomos, en la medida en que la red social ya se encuentra creada y no resulta necesario generar una nueva plataforma para consumir la conducta.

Tabla 2. *Iter Criminis* Clásico vs. *Iter Criminis* Digital según la Ley N.º 30096.

Fase del <i>Iter Criminis</i>	Modelo Clásico	Entorno Digital (Ley 30096)	Criterio Dogmático de Relevancia Penal
Fase interna (<i>cogitaciones</i>)	Actos puramente mentales. No existe exteriorización del plan.	Igual: la deliberación interna no deja huella digital ni genera riesgo técnico.	No punible. Derecho penal de acto (art. 2.24.d Const.).
Actos preparatorios	Generalmente impunes por su ambigüedad y ausencia de riesgo concreto.	Aparición de conductas técnicas: creación o posesión de <i>malware</i> , IP <i>spoofing</i> , escaneo de puertos, ingeniería social inicial. Algunos son punibles (art. 10).	Relevancia penal excepcional cuando existe riesgo cualificado y finalidad inequívoca.
Inicio de ejecución	Realización del primer acto	Activación directa del ataque:	“Interacción directa con el

Fase del <i>Iter Criminis</i>	Modelo Clásico	Entorno Digital (Ley 30096)	Criterio Dogmático de Relevancia Penal
(tentativa)	directamente vinculado al tipo penal.	ejecución de <i>scripts</i> , despliegue de fuerza bruta, envío masivo de <i>phishing</i> , interacción con el sistema objetivo. Cifrado de datos, acceso no autorizado, manipulación de información, captura de credenciales, afectación a la confidencialidad, integridad o disponibilidad (CID).	sistema”: se activa un proceso técnico con potencial inmediato de afectación. Se materializa el resultado típico: vulneración de CID o desplazamiento patrimonial automatizado.
Consumación	Lesión o puesta en peligro conforme al tipo penal.		

Nota. Fuente: Valdera (2025). Elaboración a partir de la sistematización dogmática de las fases del *iter criminis* clásico y su reconfiguración en los delitos informáticos previstos en la Ley N.º 30096, con base en la doctrina citada en la Introducción y en la jurisprudencia sistematizada en la tabla 1.

La tabla 2 permite visualizar cómo el entorno digital comprime las fases del delito y exige criterios funcionales más precisos para delimitar la relevancia penal de cada una. En la fase interna (*cogitaciones*), el modelo clásico y el entorno digital coinciden en que se trata de actos puramente mentales sin exteriorización, de modo que el criterio de relevancia penal sigue siendo la impunidad absoluta que impone el derecho penal de acto (art. 2.24.d de la Constitución). En los actos preparatorios, el entorno digital introduce conductas técnicas específicas, como la creación o posesión de *malware*, el IP *spoofing* o el escaneo de puertos, algunas de las cuales, a diferencia del modelo clásico, resultan punibles conforme al artículo 10 de la Ley N.º 30096 cuando revelan un riesgo cualificado y una finalidad inequívoca.

El inicio de ejecución o tentativa se manifiesta digitalmente en la activación directa del ataque, como la ejecución de *scripts* o el envío masivo de *phishing*, momento en que se activa un proceso técnico con potencial inmediato de afectación al bien jurídico. Finalmente, la consumación se materializa mediante el cifrado de datos, el acceso no autorizado o la captura de credenciales, es decir, con la vulneración efectiva de la confidencialidad, integridad o disponibilidad de los datos, o con el desplazamiento patrimonial automatizado.

4. Discusión

Los resultados expuestos permiten sostener que el modelo clásico del *iter criminis* conserva utilidad conceptual, pero requiere criterios funcionales adicionales para operar en el entorno digital. Esta conclusión coincide con la línea sostenida por Zhou et al. (2024), para quienes la automatización y la deslocalización tecnológica comprimen las fases del delito sin eliminar la exigencia constitucional de exteriorización de la conducta. A diferencia de posturas más restrictivas, que consideran que cualquier adelantamiento de la punibilidad de actos preparatorios digitales vulnera *per se* el derecho penal de acto, los resultados sugieren que dicho adelantamiento resulta constitucionalmente admisible siempre que se acredite un riesgo cualificado y una finalidad inequívoca.

El hallazgo empírico según el cual la Corte Suprema peruana no ha publicado jurisprudencia que aplique de manera específica las categorías del *iter criminis* a los ciberdelitos de la Ley N.º 30096, concentrándose la jurisprudencia general disponible (tabla 1) en los aspectos probatorios y procesales, confirma que identificar teóricamente las fases del delito es tarea distinta de probarlas ante un tribunal: la naturaleza del ciberespacio impone retos formidables a la justicia penal peruana, que se examinan a continuación.

4.1. Los Desafíos Probatorios en la Acreditación del *Iter Criminis* Digital

Los resultados evidencian que la identificación teórica de las fases del *iter criminis* digital constituye solo una parte del problema. En la práctica judicial, el mayor desafío no radica en definir cuándo una conducta informática deja de ser preparatoria para convertirse en ejecutiva, sino en acreditar procesalmente esa transición ante un tribunal. A continuación, se examinan cuatro desafíos probatorios centrales para la persecución penal de los ciberdelitos: la volatilidad de la evidencia digital, la cadena de custodia especializada, el rol de la pericia informática forense y la cooperación judicial

internacional.

4.1.1. La Evidencia Digital: Volatilidad y Preservación

La evidencia digital posee una característica distintiva frente a los elementos probatorios tradicionales: su extrema volatilidad. Un archivo puede ser modificado sin dejar rastro visible, los metadatos pueden alterarse de manera remota y los registros de actividad (*logs*) pueden ser borrados o sobrescritos automáticamente por el propio sistema. Al respecto, Ofori y Akoto (2020) y Garfinkel (2009) coinciden en que la fragilidad de la información digital exige una actuación inmediata, técnica y jurídicamente adecuada para evitar su pérdida o contaminación.

Acreditar la preparación o ejecución de un ciberdelito implica identificar artefactos digitales que revelen el comportamiento del agente, como fragmentos de código, historiales de navegación, correos de planificación o instrucciones de ejecución. Estos elementos pueden desaparecer en segundos, no solo por acción del sospechoso, sino también por procesos automáticos de los sistemas operativos o servidores. Ante esta realidad, la primera actuación del fiscal debe dirigirse a obtener una medida urgente de preservación de datos.

El Convenio de Budapest, ratificado por el Perú, permite ordenar a los proveedores de servicios de internet la conservación inmediata de registros digitales mientras se tramita una solicitud de entrega o incautación. Como explican Casino et al. (2022), esta medida funciona como un “congelamiento temporal” de la evidencia para impedir que el transcurso del tiempo o la acción del autor frustren la investigación.

La búsqueda de jurisprudencia realizada para este estudio no permitió identificar pronunciamientos de la Corte Suprema peruana que aborden específicamente la preservación temprana de la evidencia digital en delitos informáticos, lo que constituye en sí mismo un indicio del rezago de la práctica judicial peruana frente a la dinámica técnica de la ciberdelincuencia. La doctrina especializada aporta, sin embargo, un matiz adicional.

En efecto, Lewulis (2022) vincula la preservación temprana con la integridad posterior de la cadena de custodia y con la prevención de nulidades probatorias, de modo que la oportunidad de la medida condiciona no solo la conservación del dato, sino también su valor en juicio.

4.1.2. La Cadena de Custodia en el Entorno Digital

La validez de la evidencia digital en el proceso penal depende de una cadena de custodia rigurosa, capaz de acreditar que la información obtenida no ha sido alterada desde su incautación hasta su incorporación al juicio. A diferencia de la evidencia física, la información digital puede modificarse de manera imperceptible, por lo que su manipulación debe seguir protocolos estrictos. Siguiendo a Ofori y Akoto (2020) y a Garfinkel (2009), la cadena de custodia digital exige documentar cada intervención técnica, así como el estado exacto en que se encontraba el archivo, dispositivo o registro incautado.

La herramienta central para garantizar esta integridad son las funciones *hash*, firmas criptográficas irrepetibles que permiten verificar que un archivo no ha sufrido modificaciones. El perito debe generar el *hash* durante la clonación forense del dispositivo, conservarlo como referencia y, posteriormente, verificarlo cada vez que se accede a la copia pericial: si el *hash* inicial y el *hash* de verificación coinciden, se acredita que la evidencia mantiene su integridad absoluta; de lo contrario, la prueba se considera contaminada.

La jurisprudencia peruana reciente respalda esta exigencia, con matices. En la Apelación N.º 77-2024 (Corte Suprema, Sala Penal Permanente, 5 de noviembre de 2024), la Corte sostuvo, respecto de evidencia de audio y video, que el perito ha de recibir los archivos informáticos acompañados de su código *hash* y, si este no existe, debe generar un código de aseguramiento digital, reconociendo el *hash* como mecanismo idóneo para garantizar la autenticidad de la evidencia digital. Sobre la cadena de custodia, la Casación N.º 1669-2021-Loreto (Sala Penal Permanente, 2023) precisó que las irregularidades, por sí solas, no suponen una afectación de derechos

fundamentales, salvo que revistan tal gravedad que configuren una ruptura de la cadena de custodia, criterio reafirmado por el Recurso de Nulidad N.º 1714-2023-Lima Sur (Sala Penal Transitoria, 12 de agosto de 2024), que calificó dicha ruptura como un acto irregular que no acarrea de manera automática la nulidad o inutilización de la prueba.

Estos criterios, aunque ajenos al contexto específico de la ciberdelincuencia, son directamente aplicables a la evidencia digital: no toda irregularidad invalida la prueba, solo aquella de gravedad sustancial. El cumplimiento riguroso de estos protocolos sigue siendo, no obstante, la vía más segura para asegurar la validez probatoria de registros de redes sociales, correos electrónicos, *logs* de servidores y dispositivos de almacenamiento; un error grave en cualquiera de estas etapas puede debilitar el sustento probatorio de la acusación fiscal.

4.1.3. El Rol de la Pericia Informática Forense

La investigación de los ciberdelitos requiere un nivel de especialización técnica que excede el conocimiento jurídico tradicional. Por ello, el perito informático forense se convierte en un actor fundamental dentro del proceso penal, al servir como puente entre la complejidad tecnológica y la función jurisdiccional. A juicio de Ofori y Akoto (2020), el perito no solo identifica, recupera y analiza evidencia digital, sino que también la interpreta y la traduce a un lenguaje comprensible para fiscales y jueces, garantizando que la prueba técnica pueda ser evaluada conforme a los estándares procesales.

Mediante herramientas especializadas, el perito puede reconstruir acciones ejecutadas en un sistema, recuperar archivos eliminados, analizar tráfico de red, correlacionar eventos con sellos de tiempo y determinar la activación de *malware* o el origen de una transferencia ilícita. Este trabajo resulta determinante para establecer si la conducta corresponde a actos preparatorios, tentativa o consumación, pues, como destaca Garfinkel (2009), la temporalidad y la trazabilidad digitales son

esenciales para reconstruir el *iter criminis* en el entorno informático.

Aunque no se identificó jurisprudencia suprema peruana específica sobre delitos informáticos en este punto, sí existe un criterio general aplicable por analogía. En el Recurso de Nulidad N.º 7-2021-Puno (6 de octubre de 2021), la Corte Suprema anuló una sentencia por presentar una deficiencia estructural en su motivación respecto de la apreciación conjunta de la prueba, al haberse omitido valorar la pericia contable de manera integral y contextualizada. Aunque se trata de un caso de peculado, este criterio es trasladable a la pericia informática forense: la valoración parcial de un análisis pericial invalida la acreditación de los hechos, dada la naturaleza altamente técnica y volátil de la evidencia digital. El rol del perito también se encuentra respaldado por estándares internacionales como la ISO/IEC 27037 y la ISO/IEC 27041, que orientan la actuación pericial para asegurar hallazgos reproducibles y verificables en juicio. En este contexto, el perito informático forense no es un actor accesorio, sino un elemento estructural para acreditar las fases del delito digital.

4.1.4. La Cooperación Judicial Internacional y el Convenio de Budapest

La naturaleza transnacional de la ciberdelincuencia convierte a la cooperación judicial internacional en un componente indispensable para la acreditación del *iter criminis* digital. Los ataques informáticos rara vez se circunscriben a un solo territorio: un autor puede operar desde un país, utilizar infraestructura alojada en otro y afectar directamente a víctimas en el Perú. Según Zhou et al. (2024) y Dragojlović (2023), esta dispersión geográfica fragmenta la evidencia digital y exige mecanismos de coordinación capaces de superar las fronteras estatales y la diversidad normativa, conforme a los estándares internacionales y nacionales de jurisdicción aplicables a la ciberdelincuencia.

El Convenio de Budapest sobre Ciberdelincuencia, ratificado por el Perú, constituye el

principal instrumento internacional para enfrentar estos desafíos, al establecer procedimientos ágiles para la preservación expedita de datos, la entrega transfronteriza de registros digitales y la asistencia mutua entre autoridades. Entre ellos figuran la conservación rápida de datos almacenados (art. 16) y la conservación y revelación parcial de datos de tráfico (art. 17), cuya relevancia como primera actuación fiscal se expuso en el apartado 4.1.1. (La Evidencia Digital: Volatilidad y Preservación).

No obstante, la cooperación judicial internacional enfrenta limitaciones prácticas. En el plano operativo, Casino et al. (2022) advierten que la diferencia entre sistemas jurídicos, los plazos de respuesta de autoridades extranjeras y la diversidad de estándares probatorios pueden obstaculizar una investigación, hallazgo que coincide con lo documentado por Novak (2022) sobre la admisibilidad heterogénea de la evidencia digital en distintas jurisdicciones, y con la constatación de Bigos (2005) sobre la dificultad estructural de fijar jurisdicción frente a agravios transfronterizos ocurridos en internet.

No se identificó jurisprudencia suprema peruana que reconozca expresamente esta problemática en materia de ciberdelitos, un vacío adicional frente a un desafío que la doctrina documenta con consistencia: la eficacia de la persecución penal depende, en buena medida, de la rapidez con la que otros países atiendan las solicitudes de preservación o entrega de datos. En este escenario, el desafío para el sistema penal peruano no radica solo en la existencia del marco jurídico internacional, sino en la capacidad institucional para activarlo oportunamente.

4.2. El *Iter Criminis* Digital en el Derecho Comparado

La reinterpretación del *iter criminis* en contextos informáticos no es un desafío exclusivo del ordenamiento peruano. La doctrina y la jurisprudencia comparadas han empezado a desarrollar criterios funcionales que permiten delimitar con mayor precisión los actos preparatorios punibles, el inicio de ejecución digital y la

consumación en delitos informáticos.

En el caso español, el Tribunal Supremo ha establecido que el despliegue de herramientas automatizadas, como la ejecución de *malware* o el lanzamiento de ataques de fuerza bruta, constituye inicio de ejecución cuando activa un proceso técnico idóneo para vulnerar un sistema, aunque no haya producido aún la afectación final. La jurisprudencia europea también ha enfatizado que la mera posesión de herramientas informáticas no basta para la punibilidad, salvo que exista un riesgo cualificado que revele finalidad delictiva inequívoca, criterio recogido tanto en el Convenio de Budapest como en la Directiva 2013/40/UE.

En Chile, la Ley N.º 21.459, publicada el 20 de junio de 2022, sanciona ciertos actos preparatorios digitales siempre que exista peligro concreto para la integridad de los sistemas; la doctrina profesional señala que en delitos como la intrusión informática la tentativa puede configurarse incluso con la sola interacción inicial entre el agente y la plataforma objetivo. En Argentina, la literatura penal plantea que la delimitación entre preparación y ejecución debe centrarse en el “riesgo automatizado” propio de los sistemas informáticos. Este breve panorama evidencia que los ordenamientos comparados convergen en dos tendencias: la adopción de criterios funcionales para determinar el inicio de ejecución digital, y la punición excepcional de actos preparatorios solo cuando generan un riesgo cualificado verificable, criterios útiles para consolidar una dogmática coherente del *iter criminis* digital en el sistema penal peruano.

Frente a estas tendencias, el ordenamiento peruano muestra un desarrollo menor: los tipos penales relativos a la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos (CID) no han sido desarrollados en el sistema penal peruano con la precisión técnica deseable. El preámbulo del Convenio de Budapest sobre la Ciberdelincuencia (23 de noviembre de 2001) y la Directiva (UE) 2016/1148 (posteriormente derogada y sustituida por la Directiva (UE) 2022/2555, conocida como NIS2), que en su

artículo 4 delimita la seguridad de las redes y sistemas de información, evidencian la necesidad de que los Estados consoliden una política común. La legislación peruana debería avanzar en un sentido similar, pues carece de una norma integral sobre tratamiento de datos digitales, seguridad y obligaciones de los operadores de servicios esenciales y digitales, aspecto trascendental para definir el bien jurídico de la criminalidad de ataque contra los sistemas de información.

5. Conclusiones

El presente trabajo ofrece cuatro aportes principales a la dogmática penal peruana en materia de ciberdelincuencia, sustentados en el análisis normativo, doctrinal y jurisprudencial de las tablas 1 y 2, incluida la sistematización de siete resoluciones de la Corte Suprema aplicables por analogía ante la ausencia verificada de jurisprudencia específica sobre la materia. En primer lugar, propone un criterio funcional para identificar el inicio de ejecución digital, basado en la activación de un proceso técnico idóneo capaz de generar una afectación inmediata o altamente probable al bien jurídico.

En segundo lugar, desarrolla una reinterpretación del acto preparatorio punible en el entorno informático, distinguiendo entre conductas técnicamente neutrales y aquellas que revelan un riesgo cualificado y una finalidad delictiva inequívoca. En tercer lugar, formula criterios para delimitar la tentativa digital, especialmente en delitos cuya ejecución se automatiza tras un solo clic. Finalmente, aporta un marco operativo para fiscales y jueces, orientado a mejorar la identificación de las fases del *iter criminis* digital y la valoración de la evidencia informática, con énfasis en la preservación de metadatos, la cadena de custodia y la pericia técnica especializada.

Como aspecto novedoso, el estudio documenta el vacío jurisprudencial supremo sobre el *iter criminis* en los ciberdelitos de la Ley N.º 30096, lo que permite afirmar que, si bien la teoría clásica del *iter criminis* mantiene vigencia como marco conceptual del derecho penal

peruano, su aplicación al entorno digital exige tanto una reformulación interpretativa como un mayor desarrollo jurisprudencial específico por parte de la Corte Suprema.

Este artículo aporta a la ciencia jurídica peruana una sistematización dogmática actualizada del *iter criminis* digital. Desde una perspectiva práctica, los hallazgos tienen implicancias directas para fiscales, jueces y operadores de justicia: la identificación del inicio de ejecución en ciberdelitos requiere abandonar criterios puramente materiales y adoptar parámetros funcionales basados en la activación del riesgo digital, en delitos como el acceso ilícito, el fraude informático o la suplantación de identidad, donde un solo clic puede activar un proceso automatizado con capacidad de causar daño inmediato.

Entre las limitaciones del presente estudio se encuentra el alcance de su corpus documental: al tratarse de un análisis cualitativo de fuentes normativas, doctrinales y de siete resoluciones de la Corte Suprema, no se incorporaron datos sobre la frecuencia real con la que fiscales y jueces peruanos aplican los criterios funcionales aquí propuestos en casos concretos, aspecto que futuras investigaciones podrían abordar mediante el análisis de expedientes fiscales y judiciales o entrevistas a operadores de justicia.

A ello se suma la escasez de jurisprudencia suprema peruana específica sobre ciberdelitos, evidenciada en el proceso de búsqueda documental, que obligó a construir buena parte del análisis mediante la extensión analógica de criterios generales del *iter criminis*, con las cautelas interpretativas que ello supone. Asimismo, el análisis se circunscribió a los tipos penales vigentes de la Ley N.º 30096, sin abarcar de manera exhaustiva otras figuras del Código Penal peruano que también podrían cometerse por medios informáticos.

El estudio identifica, además, vacíos normativos relevantes en la Ley N.º 30096. Entre ellos destacan la ausencia de criterios normativos claros para diferenciar actos preparatorios digitales de actos ejecutivos, la falta de regulación sobre la responsabilidad por riesgos automatizados, la inexistencia de definiciones técnicas

vinculantes para operadores de justicia y la insuficiente previsión normativa sobre la preservación obligatoria de metadatos, registros de conexión y trazabilidad digital por parte de proveedores de servicios tecnológicos.

Estos vacíos incrementan la incertidumbre interpretativa y debilitan la eficacia persecutoria del sistema penal. En consecuencia, se recomienda fortalecer la Ley N.º 30096 mediante reformas orientadas a incorporar definiciones técnicas precisas sobre las fases del *iter criminis* digital, establecer deberes legales reforzados de conservación y entrega de evidencia digital por parte de proveedores tecnológicos, regular explícitamente el concepto de “riesgo automatizado” como umbral para delimitar la tentativa digital, y ampliar el catálogo de actos preparatorios punibles únicamente cuando exista un peligro cualificado comprobable para la confidencialidad, integridad o disponibilidad de datos.

El estudio concluye que los mayores obstáculos para acreditar el *iter criminis* digital no son conceptuales, sino tecnológicos y probatorios: la volatilidad de la evidencia digital exige una actuación fiscal inmediata, la preservación urgente de información y un manejo estricto de la cadena de custodia digital, sin los cuales la investigación penal queda seriamente comprometida. De igual modo, la dimensión transnacional de la ciberdelincuencia demanda una aplicación más eficiente del Convenio de Budapest y una capacidad institucional fortalecida para gestionar solicitudes de cooperación internacional.

Como línea futura de investigación, se recomienda que el Estado peruano adopte una política criminal digital moderna, basada en inversión tecnológica, capacitación permanente de operadores de justicia y adopción de criterios dogmáticos uniformes, y que estudios posteriores, con muestras amplias de expedientes fiscales y judiciales, contrasten los criterios funcionales aquí propuestos con la práctica judicial efectiva, a fin de asegurar una persecución penal eficaz y respetuosa de las garantías constitucionales en un entorno donde la criminalidad evoluciona con mayor rapidez que el derecho.

6. Referencias

- Aksamitowska, K. (2021). Digital evidence in domestic core international crimes prosecutions: Lessons learned from Germany, Sweden, Finland and the Netherlands. *Journal of International Criminal Justice*, 19(1), 189–211. <https://doi.org/10.1093/jicj/mqab035>
- Al-Faraji, N. M. L. (2025). The legal framework of cybercrime and the obstacles to proving it. *International Journal of Criminal, Common and Statutory Law*, 5(1), 15–21. <https://doi.org/10.22271/27899497.2025.v5.i1a.113>
- Alhawawsheh, A., Alfalahi, Q., Soltan, K., Taher, A., & Dhaheri, L. (2025). Digital evidence as a means of proof in criminal proceedings in the UAE. *Access to Justice in Eastern Europe*, 8(3), 521–540. <https://doi.org/10.33327/AJEE-18-8.3-a000111>
- Alluqmani, K., Karrar, A. E., Alhaidari, M., Alharbi, R., & Alharbi, S. (2025). Assessing the efficacy of security awareness training in mitigating phishing attacks: A review. *International Journal of Advanced Trends in Computer Science and Engineering*, 14(3), 177–184. <https://doi.org/10.30534/ijatcse/2025/081432025>
- Bein, D. (1993). Preparatory offences. *Israel Law Review*, 27(1-2), 185–212. <https://doi.org/10.1017/s0021223700016903>
- Bigos, O. (2005). Jurisdiction over cross-border wrongs on the Internet. *International & Comparative Law Quarterly*, 54(3), 585–620. <https://doi.org/10.1093/icql/lei019>
- Caputo, D. D., Pflieger, S. L., Freeman, J. D., & Johnson, M. E. (2014). Going spear phishing: Exploring embedded training and awareness. *IEEE Security & Privacy*, 12(1), 28–38. <https://doi.org/10.1109/MSP.2013.106>
- Casino, F., Pina, C., López-Aguilar, P., Batista, E., Solanas, A., & Patsakis, C. (2022). SoK: Cross-border criminal investigations and digital evidence. *Journal of Cybersecurity*, 8(1), tyac014. <https://doi.org/10.1093/cybsec/tyac014>
- Cohen, L., Manion, L., & Morrison, K. (2018). *Research methods in education* (8th ed.). Routledge.
- Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.
- Cross, C., & Blackshaw, D. (2015). Improving the police response to online fraud. *Policing: A Journal of Policy and Practice*, 9(2), 119–128. <https://doi.org/10.1093/polic/pau044>
- Das, A., Baki, S., El Aassal, A., Verma, R. M., & Dunbar, A. (2020). SoK: A comprehensive reexamination of phishing research from the security perspective. *IEEE Communications Surveys & Tutorials*, 22(1), 671–708. <https://doi.org/10.1109/COMST.2019.2957750>
- Dragojlović, J. (2023). Jurisdiction for criminal offenses of cybercrime: International and national standards. *Pravo - teorija i praksa*, 40(Suppl.), 63–83. <https://doi.org/10.5937/ptp2300063D>
- Garfinkel, S. L. (2009). Providing cryptographic security and evidentiary chain-of-custody with the Advanced Forensic Format, Library, and Tools. *International Journal of Digital Crime and Forensics*, 1(1), 1–28. <https://doi.org/10.4018/JDCF.2009010101>
- Greene, K., Steves, M., & Theofanos, M. (2018). No phishing beyond this point. *Computer*, 51(6), 86–89. <https://doi.org/10.1109/MC.2018.2701632>
- Hernández-Sampieri, R., & Mendoza, C. P. (2018). *Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta*. McGraw-Hill Interamericana Editores.
- Hutchings, A., Clayton, R., & Anderson, R. (2016). Taking down websites to prevent crime. 2016 APWG Symposium on Electronic Crime Research (eCrime), 1–10. <https://doi.org/10.1109/ECRIME.2016.7487947>
- Ingemarsson, J., Birath, M., & Kävrestad, J. (2025). Factors influencing Swedish citizens' willingness to provide their mobile phones to forensic examination. *International Journal of Information Security*, 24(1), 42. <https://doi.org/10.1007/s10207-024-00955-4>
- Irawan, B., Mulyanti, D., Budiaman, H., Rahman, Y. M., & Taufiqurrohmah, A. (2025). Perspective of state sovereignty in law enforcement related to cyberlaw jurisdiction. *Law Reform*, 21(1), 120–134. <https://doi.org/10.14710/lr.v21i1.68760>
- Iuga, C., Nurse, J. R. C., & Erola, A. (2016). Baiting the hook: Factors impacting susceptibility to phishing attacks. *Human-Centric Computing and Information Sciences*, 6(1), 8. <https://doi.org/10.1186/s13673-016-0065-2>
- Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10), 94–100. <https://doi.org/10.1145/1290958.1290968>
- Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. *Proceedings of the 2nd Annual eCrime Researchers Summit*, 70–81. <https://doi.org/10.1145/1299015.1299022>
- Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F., & Hong, J. (2010). Teaching Johnny not to fall for phish. *ACM Transactions on Internet Technology*, 10(2), 1–31. <https://doi.org/10.1145/1754393.1754396>
- Leukfeldt, E. R., Lavorgna, A., & Kleemans, E. R. (2017). Organised cybercrime or cybercrime that is organised? An assessment of the conceptualisation of financial cybercrime as organised crime. *European Journal on Criminal Policy and Research*, 23(3), 287–300. <https://doi.org/10.1007/s10610-016-9332-z>
- Lewulis, P. (2022). Collecting digital evidence from online sources: Deficiencies in current Polish criminal law. *Criminal Law Forum*, 33(1), 39–62. <https://doi.org/10.1007/s10609-021-09430-4>

- Logos, K., Brewer, R., Langos, C., & Westlake, B. (2023). Establishing a framework for the ethical and legal use of web scrapers by cybercrime and cybersecurity researchers: Learnings from a systematic review of Australian research. *International Journal of Law and Information Technology*, 31(3), 186–212. <https://doi.org/10.1093/ijlit/eaad023>
- Novak, M. (2022). Digital evidence in appeals of criminal cases before the U.S. courts of appeal: A review of decisions and examination of the legal landscape from 2016-2020. *Journal of Digital Forensics, Security and Law*, 17(1), 3. <https://doi.org/10.15394/jdfs.2022.1734>
- Ofori, A. Y., & Akoto, D. (2020). Digital forensics investigation jurisprudence: Issues of admissibility of digital evidence. *Journal of Forensic, Legal & Investigative Sciences*, 6(1), 1–8. <https://doi.org/10.24966/FLIS-733X/100045>
- Sheng, S., Holbrook, M., Kumaraguru, P., Cranor, L. F., & Downs, J. S. (2010). Who falls for phish?. A demographic analysis of phishing susceptibility and effectiveness of interventions. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI '10)*, 373–382. <https://doi.org/10.1145/1753326.1753383>
- Sousa-Silva, R. (2024). We attempted to deliver your package: Forensic translation in the fight against cross-border cybercrime. *International Journal for the Semiotics of Law - Revue internationale de Sémiotique juridique*, 37(4), 1323–1349. <https://doi.org/10.1007/s11196-023-10102-2>
- Sutter, T., Bozkir, A. S., Gehring, B., & Berlich, P. (2022). Avoiding the hook: Influential factors of phishing awareness training on click-rates and a data-driven approach to predict email difficulty perception. *IEEE Access*, 10, 100540–100565. <https://doi.org/10.1109/ACCESS.2022.3207272>
- Wang, X. (2025). Global (re-)framing of cybercrime: An emerging common interest in flux of competing normative powers?. *Leiden Journal of International Law*, 38(2), 235–261. <https://doi.org/10.1017/S0922156524000402>
- Zhou, Y., Tiwari, M., Bernot, A., & Lin, K. (2024). Metacrime and cybercrime: Exploring the convergence and divergence in digital criminality. *Asian Journal of Criminology*, 19(3), 419–439. <https://doi.org/10.1007/s11417-024-09436-y>

Reseña biográfica del autor

Juan Eduardo Valdera Olivos | jvalderao@ucvvirtual.edu.pe

Es abogado, magíster en Ciencias Penales por la Universidad Nacional Pedro Ruiz Gallo (Lambayeque, Perú) y doctorando en Gestión Pública en la Universidad César Vallejo (Chiclayo, Perú). Cuenta con más de quince años de trayectoria en la Corte Superior de Justicia de Lambayeque, donde se ha desempeñado como especialista judicial y como juez supernumerario, cargo en el que obtuvo reconocimientos institucionales por su productividad jurisdiccional. Su línea de investigación se centra en el derecho penal informático, la dogmática del *iter criminis* y los desafíos probatorios de la ciberdelincuencia en el ordenamiento jurídico peruano.

Agradecimientos. El autor expresa su agradecimiento a la Universidad César Vallejo (UCV), sede Chiclayo, Perú, por el respaldo académico e institucional brindado durante el desarrollo de la presente investigación.

Declaraciones del autor

Contribución del autor (Taxonomía CRediT). Juan Eduardo Valdera Olivos: Conceptualización, Curación de datos, Análisis formal, Investigación, Metodología, Administración del proyecto, Recursos, Validación, Visualización, Escritura - borrador original, Escritura - revisión y edición.

Financiamiento. La presente investigación no contó con financiamiento externo de ninguna entidad pública o privada; fue realizada con recursos propios del autor.

Conflicto de intereses. El autor declara no tener ningún conflicto de interés real, potencial o percibido en relación con la investigación, autoría o publicación de este artículo.

Declaración de disponibilidad de datos. El estudio no generó bases de datos primarias. El corpus analizado está compuesto por fuentes normativas y doctrinales citadas en el texto y por siete resoluciones de la Corte Suprema del Perú de acceso público, identificadas en la tabla 1 con su número de expediente y año, lo que permite su consulta directa en el sistema de jurisprudencia del Poder Judicial del Perú.

Declaración de uso de Inteligencia Artificial. Durante la corrección editorial de este manuscrito se empleó el asistente de inteligencia artificial Claude (Anthropic) como herramienta de apoyo para la revisión de citas y referencias conforme a las normas APA (7.^a ed.) y la corrección lingüística y de estilo. La herramienta no se utilizó para generar datos, seleccionar las fuentes ni realizar el análisis jurisprudencial. El autor revisó y validó la totalidad del contenido resultante y asume plena responsabilidad por su exactitud académica y jurídica.

Aprobación ética y consentimiento informado. La presente investigación no involucró la participación de seres humanos como sujetos de estudio ni el tratamiento de datos personales identificables, en tanto se trató de un análisis documental cualitativo basado exclusivamente en el examen de fuentes normativas, doctrinales y jurisprudenciales de acceso público, por lo que no fue necesaria la aprobación de un comité de ética institucional ni la obtención de consentimiento informado.