El hurto por medios informáticos en Colombia según la Ley 1273 de 2009. Alcances y limitaciones durante el periodo 2022 -2025

Facultad de Derecho
Universidad Autónoma Latinoamericana

El hurto por medios informáticos en Colombia según la Ley 1273 de 2009. Alcances y limitaciones durante el periodo 2022 -2025

Evelin Carvajal Torres
Salomé Duarte
Mayo 2026

Facultad de Derecho
Universidad Autónoma Latinoamericana

Contenido

Lista de abreviaturas y acrónimos

A

ADC 51. *Ação Declaratória de Constitucionalidade No. 51*
AIDP. *Asociación Internacional de Derecho Penal*

B

BNFE. *Base Nacional de Fraudes Bancárias Eletrônicas*

C

CFAA. *Computer Fraud and Abuse Act*
CSIRT- CL. *Centro de Respuesta a Incidentes de Seguridad Informática de Chile*
CSJ. *Corte Suprema de Justicia*
CT-Y. *Cybercrime Convention Committee*

D

DANE. *Departamento Administrativo Nacional de Estadística*
DDoS. *Denegación de Servicios Distribuida*
DHS. *Department of Homeland Security*

E

ENCS. *Estrategia Nacional de Ciberseguridad*

F

FEBRABAN. *Federación Brasileña de Bancos*
FGN. *Fiscalía General de la Nación*

I

IA. *Inteligencia Artificial*

L

LGPD. *Ley General de Protección de Datos*

N

NSA. *National Security Agency*

O

OCDE. *Organización para la Cooperación y el Desarrollo Económicos*
ONU. *Organización de las Naciones Unidas*

R

R3D. *Red en Defensa de los Derechos Digitales*

S

STF. *Supremo Tribunal Federal*

U

UCIEX. *Unidad de Cooperación Internacional y Extradiciones*
UGEPT. *Unidad de Gobierno Electrónico*
ULDECO. *Unidad de Lavado de Dinero, Delitos Económicos, Medioambientales y Cibercrimen*
US – CERT. *United States Computer Emergency Readiness Team*

Resumen

El presente estudio delimita su objeto de análisis en la eficacia material de la Ley 1273 de 2009 frente al delito de hurto informático en Colombia, un fenómeno condicionado por la volatilidad y fugacidad de la evidencia digital. Para ello, el marco analítico evalúa la jurisprudencia hito que ha moldeado la interpretación de dicha norma, persiguiendo el equilibrio entre la eficacia punitiva del Estado y las garantías del debido proceso. Asimismo, mediante un ejercicio de derecho comparado con Argentina, Brasil, Chile, Estados Unidos y México, la investigación demuestra que la problemática central no radica en una insuficiencia de tipicidad sustancial, sino en la debilidad de la infraestructura operativa y tecnológica.

las cifras consolidadas en 2024 confirmaron que el aumento en los registros de criminalidad informática no generó un volumen equivalente de condenas ni de restitución de bienes patrimoniales. Frente a este panorama, el estudio sostiene que la solución no radica en la hiperactividad legislativa sobre los tipos penales, sino en la instauración de una robusta gobernanza técnica. Consecuentemente, se propone un marco de acción operativo enfocado en cuatro pilares: la estandarización nacional de procedimientos de custodia digital, la articulación eficiente con entidades financieras a través de convenios preestablecidos, la formación técnica especializada y obligatoria para los operadores judiciales, y el diseño de métricas institucionales que permitan evaluar objetivamente el éxito de las investigaciones cibernéticas.

Palabras Claves: Hurto informático. Evidencia digital. Cadena de custodia. Eficacia probatoria. Gobernanza técnica.

Abstract

This study focuses its analysis on the material effectiveness of Law 1273 of 2009 in addressing the crime of computer theft in Colombia, a phenomenon conditioned by the volatility and ephemerality of digital evidence. To this end, the analytical framework evaluates landmark jurisprudence that has shaped the interpretation of this law, seeking a balance between the State's punitive effectiveness and the guarantees of due process. Furthermore, through a comparative law analysis with Argentina, Brazil, Chile, the United States, and Mexico, the research demonstrates that the central problem lies not in a lack of substantive legal definition of the crime, but rather in the weakness of the operational and technological infrastructure.

The consolidated figures for 2024 confirmed that the increase in reported cybercrime cases did not generate a corresponding increase in convictions or the restitution of stolen assets. Given this situation, the study argues that the solution lies not in excessive legislation on criminal offenses, but rather in the establishment of robust technical governance. Consequently, it proposes an operational framework focused on four pillars: national standardization of digital custody procedures, efficient coordination with financial institutions through pre-established agreements, specialized and mandatory technical training for judicial officers, and the design of institutional metrics to objectively evaluate the success of cybercrime investigations.

Keywords: Cyber theft. Digital evidence. Chain of custody. Evidentiary value. Technical governance

Introducción

Actualmente, gran parte de nuestras actividades diarias se realizan a través de medios digitales, como las plataformas bancarias, redes sociales y servicios en línea. Aunque esto ha facilitado la comunicación y el acceso a la información, también ha aumentado los riesgos de sufrir delitos informáticos, entre ellos el hurto informático, que consiste en obtener dinero, datos o información de manera ilegal utilizando herramientas tecnológicas. Para enfrentar esta problemática surge la Ley 1273 de 2009, en cuyo instrumento normativo se típica por primera vez los delitos informáticos en Colombia, no obstante, después de una década de existencia, al hacerse una medición sobre la eficacia de la misma ley ha dejado en el "aire" muchos interrogantes, como lo es: ¿Qué tan efectiva ha sido la aplicación de la Ley 1273 de 2009 frente al hurto informático en Colombia durante el periodo comprendido entre 2022 y 2025? Así es como por medio de esta investigación se ha propuesto responder a este interrogante, desde el desarrollo normativo como su aplicación en tribunales, Fiscalía y Policía Nacional. Por tales razones, se deben revisar estadísticas estatales sobre denuncias, fallos jurisprudenciales relevantes y las buenas prácticas institucionales desarrolladas durante los últimos años. Igualmente, esta investigación se justifica porque el hurto informático se ha convertido en una de las principales amenazas para el patrimonio económico de los ciudadanos en un contexto donde gran parte de las actividades financieras y administrativas se realizan por medios digitales. Aunque Colombia cuenta con la Ley 1273 de 2009 para sancionar este tipo de conductas, el aumento de los delitos informáticos y los constantes ciberataques a entidades públicas y privadas han puesto en evidencia que todavía existen dificultades para investigar, probar y sancionar eficazmente a los responsables. Por ello, resulta necesario analizar si la norma ha logrado cumplir su finalidad en la práctica o si existen obstáculos institucionales y técnicos que limitan su efectividad.

En este contexto, la importancia de este estudio radica en que no se centra únicamente en el análisis de la ley, sino también en la forma en que esta se aplica dentro del sistema penal colombiano. A través del examen de decisiones judiciales, estadísticas y documentos institucionales correspondientes al periodo 2021-2025, se busca identificar las principales dificultades relacionadas con la obtención de pruebas digitales, la capacidad técnica de las autoridades y la coordinación entre las entidades encargadas de la investigación. De esta manera, la investigación pretende aportar elementos que contribuyan al fortalecimiento de la respuesta estatal frente al hurto informático y a una mejor protección de los derechos patrimoniales y de la información de los ciudadanos.

por tal razón nos planteamos como objetivo general realizar un análisis sobre los alcances y límites de la Ley 1273 de 2009 en la sanción del hurto informático en Colombia para desarrollarlo, estructuramos tres propósitos específicos:

1.Analizar la evolución del régimen penal colombiano en materia de delitos informáticos, particularmente del hurto informático, y el tratamiento jurisprudencial de la Ley 1273 de 2009.

2. Evaluar la eficacia material de los tipos penales previstos en la Ley 1273 de 2009 frente al hurto informático a través del estudio de la labor de la FGN y la judicatura, estableciendo si las herramientas actuales implementadas por tales instituciones son suficientes para demostrar las conductas de hurto informático ante los tribunales, y por ende, ser sancionadas.

3.Comparar los marcos normativos y procesales del hurto informático en Argentina, Brasil, Chile, Estados Unidos y México, con el fin de identificar buenas prácticas aplicables al contexto colombiano.

Como marco teórico realizamos revisión de la literatura que muestra que el crecimiento de las tecnologías digitales ha venido acompañado de un aumento de los delitos informáticos, especialmente

del hurto por medios informáticos. Diversos autores coinciden en que este fenómeno representa un desafío para el Derecho Penal, ya que las formas tradicionales de investigación y prueba no siempre son suficientes para enfrentar delitos que se cometen en entornos digitales. Además, estudios nacionales e internacionales destacan la importancia de contar con herramientas como la informática forense, el análisis de evidencia digital y la cooperación entre instituciones para lograr una persecución penal efectiva. También se evidencia que nuevas tecnologías, como la inteligencia artificial y las criptomonedas, han generado retos adicionales para la aplicación de la ley.

Por otra parte, las investigaciones revisadas coinciden en que la Ley 1273 de 2009 constituyó un avance importante en la regulación de los delitos informáticos en Colombia. Sin embargo, los principales problemas no se encuentran en la redacción de la norma, sino en su aplicación práctica. Informes recientes muestran que, aunque las denuncias por hurto informático han aumentado de manera significativa, las tasas de judicialización y condena continúan siendo bajas debido a dificultades relacionadas con la obtención de pruebas digitales, la falta de recursos técnicos especializados y la limitada capacidad institucional. En consecuencia, la literatura analizada permite concluir que la efectividad de la ley depende menos de la creación de nuevos tipos penales y más del fortalecimiento de los mecanismos de investigación, la capacitación de los operadores judiciales y la implementación de protocolos forenses adecuados.

Con el propósito de ampliar la comprensión del problema esta investigación se desarrolló mediante un enfoque con predominio cualitativo, basada en el modelo de Creswell y Plano Clark (2018), que permite unir la exploración cuantitativa con la comprensión cualitativa siguiendo un diseño secuencial que permitió combinar el análisis de datos estadísticos con la revisión jurídica y documental. En una primera etapa se analizaron cifras oficiales de la Fiscalía General de la Nación y de la Policía Nacional correspondientes al periodo 2022-2025, con el propósito de identificar tendencias relacionadas con las denuncias, la judicialización y los resultados obtenidos frente al hurto informático en Colombia. Esta información permitió establecer un panorama general sobre el comportamiento del fenómeno y la capacidad de respuesta institucional.

Posteriormente, se realizó un análisis cualitativo basado en la revisión de jurisprudencia de la Corte Suprema de Justicia y la Corte Constitucional, así como de literatura académica especializada sobre delitos informáticos. Además, se examinaron las principales dificultades procesales, probatorias e institucionales que afectan la aplicación de la Ley 1273 de 2009. Finalmente, se incorporó un estudio comparado con países como Argentina, Brasil, Chile, Ecuador y México para identificar buenas prácticas y posibles estrategias de fortalecimiento para el sistema colombiano. La información obtenida fue analizada mediante técnicas de triangulación, lo que permitió contrastar los datos estadísticos, las decisiones judiciales y los aportes doctrinales para formular conclusiones y recomendaciones con mayor nivel de confiabilidad.

Por tales razones, se puede concluir que el crecimiento de la delincuencia informática conlleva a la revisión de la Ley 1273 de 2009 frente a la creciente amenaza de la ciberdelincuencia informática en Colombia Para tales propósitos, el presente trabajo de investigación se desarrolla a lo largo de tres capítulos fundamentales que, de manera articulada, permiten comprender la complejidad del fenómeno analizado. En el primer capítulo, se abordan los fundamentos teóricos y dogmáticos, examinando la tensión existente entre el mandato normativo de la Ley 1273 de 2009 y la realidad operativa del sistema judicial, identificando las fallas estructurales en la preservación de la evidencia digital y la afectación sistemática de la cadena de custodia que han limitado la eficacia del derecho penal sustancial. Posteriormente, el segundo capítulo centra su atención en el análisis jurisprudencial y comparado, donde se examinan las posturas contradictorias de las altas cortes frente a la valoración probatoria de elementos técnicos, contrastando esta experiencia nacional con los modelos de gobernanza técnica y forense de otras jurisdicciones, lo que permite visibilizar la brecha real entre la

tipificación del delito y su procesamiento judicial efectivo. Finalmente, el tercer capítulo mediante un riguroso ejercicio de derecho comparado, que contrasta las experiencias internacionales en gobernanza técnica con las carencias del contexto colombiano, se decanta una propuesta de intervención práctica, orientada a superar el inmovilismo institucional mediante la estandarización nacional de protocolos de actuación, la formalización de convenios interinstitucionales y la capacitación continua de los operadores, permitiendo así transitar de un modelo punitivo fragmentado hacia una gobernanza técnica integral que, basada en las lecciones extraídas de otros sistemas, logre finalmente cerrar la brecha entre la tipificación del delito y su efectiva persecución y sanción en Colombia durante el periodo 2022-2025.

Capítulo 1. Contexto jurídico sobre el hurto por medios informáticos en el territorio colombiano

En el umbral de la era digital, la expansión de la conectividad reconfiguró de manera sustancial los contornos típicos del delito, al propiciar modalidades inéditas de hurto cometidas mediante sistemas informáticos. Desde la promulgación de la Ley 1273 de 2009, el sistema jurídico colombiano se vio enfrentado al reto de articular mecanismos sustantivos y procesales capaces de responder a un fenómeno que ya no podía ser comprendido desde categorías penales tradicionales. Este capítulo analiza, entre 2022 y 2025, la eficacia de dichos instrumentos en la prevención y persecución de estas conductas, apoyándose en estadísticas, decisiones judiciales y prácticas institucionales. La pregunta que estructura la investigación busca precisar hasta qué nivel estas normas[1] han sido realmente idóneas para prevenir, perseguir y reducir el hurto informático, atendiendo a su funcionamiento en los tribunales, al comportamiento de las denuncias y a la línea jurisprudencial dominante. Desde esa óptica, la investigación revisa la estructura del régimen punitivo colombiano con el propósito de valorar la respuesta del legislador frente a conductas punibles que han evolucionado desde formas simples de abuso hasta manifestaciones de alta sofisticación, mediadas por redes sociales y software malicioso.

Del examen de las estadísticas de denuncia se desprende una fractura evidente entre la respuesta normativa diseñada por el legislador y los resultados concretamente alcanzados en la práctica. Aunque la Ley 1273 de 2009 introdujo en el Código Penal un título especial orientado a proteger los bienes informáticos, el crecimiento continuo de los reportes sugiere que el problema no radica solo en la existencia de la norma, sino en las condiciones materiales y organizacionales de su aplicación. La investigación mide ese fenómeno con base en un número creciente de noticias criminales, que pasó de 65.794 denuncias en 2022 a 77.866 en 2024, y muestra vacíos operativos importantes al comprobar que el 93% de los casos no supera la etapa de indagación preliminar. Pero el estudio no se agota en la contabilidad de los hechos. El examen, además, no se circunscribe al dato bruto, sino que revisa la actuación de jueces y fiscales en la tramitación de estos procesos. No obstante, el resultado es una paradoja donde existe un sistema penal formalmente robusto que, en la práctica, ve neutralizada su capacidad de respuesta frente al hurto informático.

Seguidamente, el estudio de la jurisprudencia correspondiente a sentencias relevantes, que van desde la tipificación de hurto informático a la estafa digital hasta las que introducen agravantes por el empleo de tecnologías de ocultación, que facilitará la identificación de los modelos interpretativos vigentes en la judicatura. Esta sección cotejará los dictámenes más innovadores con la práctica usual de enmarcar estos hechos en modalidades convencionales, matizando la innovación de la Ley y revelando en diversos fallos, un desfase en la respuesta judicial ante la diversidad del delito informático.

---

[1] El régimen punitivo colombiano en esta materia se edifica sobre la **Ley 599 de 2000**, cuyo **Artículo 239** provee la estructura dogmática del hurto que sirve de soporte a la configuración del hurto informático previsto en los **artículos 269I y 269J**, hoy complementado por la **Ley 1273 de 2009**, mediante la cual se introdujo una tipificación autónoma de los ciberdelitos y se erigió el bien jurídico de la protección de la información y de los datos. En paralelo, la **Ley 906 de 2004** fija el marco para la cadena de custodia y la recolección de evidencia técnica, mientras que la **Ley 1928 de 2018** integra el **Convenio de Budapest** y habilita la cooperación internacional en materia probatoria. A ese conjunto se añaden la **Ley 2197 de 2022**, que robusteció la reacción estatal frente a la criminalidad informática, y la **Ley 2502 de 2025,** que elevó el reproche penal cuando la suplantación de identidad se comete con apoyo de inteligencia artificial.

En suma, la integración de los hallazgos criminológicos con las condiciones reales de operación y con el entorno social evidencia exigencias inaplazables para la respuesta estatal frente al hurto informático en Colombia. De manera particular, se impone perfeccionar la neutralidad tecnológica en la sanción penal, intensificar la persecución judicial y consolidar políticas criminales con orientación preventiva y restaurativa. Bajo esa premisa, este capítulo asume un papel articulador dentro del trabajo, en la medida en que trasciende la simple enumeración de vacíos y propone lineamientos de transformación normativa. Estas propuestas privilegian la formación integral de los operadores del sistema y la cooperación global como herramientas para dotar de mayor consistencia y eficacia al cuerpo normativo aplicable al delito informático en Colombia.

1.1. Transformaciones del tratamiento jurídico y respuestas penales ante el hurto informático en el contexto global

En el entorno internacional contemporáneo, los delitos informáticos se han transformado en uno de los desafíos más complejos y transversales que afectan a diversas dimensiones sociales, considerando la economía global, la seguridad interna de los Estados y el ámbito de los derechos individuales. Ante ello, tradicionalmente, los bienes jurídicos se limitaban a tutelar aspectos físicos y patrimoniales concretos; sin embargo, el avance tecnológico ha obligado a expandir esa protección hacia entornos virtuales. Dado que, este proceso plantea al Derecho Penal el reto de revisar sus categorías clásicas frente a las nuevas dinámicas digitales En tal sentido, este fenómeno exige al Derecho Penal reformular sus nociones consolidadas de acuerdo con las nuevas realidades digitales. Tal como lo expone Narváez Montenegro (2015), las legislaciones internacionales han comenzado a prevalecer la defensa de los datos personales y la intimidad, en vista de que la extracción ilícita de información puede ser tan lesiva como el apoderamiento de bienes materiales o efectivo (pp. 158 – 159). En sentido, la cimentación de un enfoque comparativo sobre el hurto informático que permite analizar los puntos de encuentro y divergencia, permitiendo diseñar estrategias normativas más eficientes y compatibles entre sí.

Frente a esta transformación de los bienes jurídicos tutelados y del escenario delincuencial, es preciso ubicar este cambio en una reconstrucción histórica del desarrollo normativo internacional, pues solo a través de una revisión de las décadas anteriores es posible advertir cómo el Derecho Internacional comenzó a sentar los cimientos de la regulación del delito informático y, de manera más específica, del hurto informático. En efecto, solo mediante una revisión de las décadas precedentes resulta posible advertir cómo el Derecho Internacional comenzó a sentar las bases de una regulación inicialmente indirecta del delito informático y, de manera más específica, de aquellas conductas que, con posterioridad, serían comprendidas dentro del fenómeno del hurto informático. En tal sentido, la comprensión contemporánea del hurto informático no puede abordarse de manera aislada ni exclusivamente desde la legislación penal interna, sino que exige una lectura histórica que permita identificar cómo el Derecho Internacional, incluso antes de conceptualizar de forma expresa la criminalidad cibernética, comenzó a consolidar categorías de protección vinculadas con activos inmateriales, contenidos digitales y formas de circulación tecnológica de información. Así ocurrió en la década de 1960, cuando se adoptaron dos convenios de especial importancia: en primer lugar, el Tratado de Roma sobre la Protección de productores de grabaciones sonoras, de 1961; y, posteriormente, el instrumento de Estocolmo de 1967, al que se atribuye el reconocimiento del valor económico y de la dimensión de propiedad intelectual de los archivos electrónicos, así como el impulso de mecanismos de cooperación internacional en la materia (Narváez Montenegro, 2015, pp. 160-161). De igual forma, en 1974 se suscribió el Convenio sobre la Distribución de Señales de Satélite, conocido como el Convenio de Bruselas (Bélgica), promovido por la Organización Mundial de la Propiedad Intelectual (OMPI) y la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), como respuesta a la retransmisión no autorizada de contenidos y a la necesidad de establecer sanciones frente a la vulneración de los derechos de autor y de los regímenes de difusión satelital (Narváez Montenegro, 2015, p. 161). Si bien esta normatividad se

concentró inicialmente en la esfera de la propiedad intelectual, no puede desconocerse que tales instrumentos operaron como antecedentes normativos de gran relevancia, en la medida en que anticiparon la necesidad de desarrollar marcos regulatorios más amplios, hoy plenamente integrados al universo de la criminalidad cibernética.

Siguiendo con el desarrollo histórico de los instrumentos jurídicos frente a la tecnología, durante la década de 1970 y 1980, diversos organismos internacionales iniciaron estudios y reuniones especializadas con el objetivo de analizar el impacto de las tecnologías de la información en el fenómeno criminal. Así fue, como en 1983, la Organización para la Cooperación y el Desarrollo Económicos (OCDE) promovió un estudio direccionado al establecimiento de estándares penales ante el empleo ilícito de programas informáticos. Por su parte, hacia 1992, la Asociación Internacional de Derecho Penal (AIDP) convocó una reunión en la ciudad alemana de Würzburg para analizar la regulación jurídica de las infracciones cibernéticas (Narváez Montenegro, 2015, pp. 160-161). Estas iniciativas demostraron que las categorías penales clásicas insuficientes y la necesidad de idear nuevas conductas punibles, al tiempo implementaban los mecanismos probatorios de colaboración internacional en la obtención de pruebas.

Como corolario de las discusiones promovidas por organismo multilaterales en las décadas previas, en 1990, en el marco del Octavo Congreso sobre Prevención del Delito y Justicia Penal de la Organización de las Naciones Unidas (ONU) en La Habana (Cuba), se dio un importante paso en la formalización del tratamiento jurídico de los delitos informáticos. A partir de este evento transnacional se establecieron tres categorías básicas en el marco de este fenómeno punitivo como son las estafas mediante alteración de sistemas informáticos, modificaciones de datos de entrada, y, afectación al software a las plataformas de almacenamiento de información. De esta manera, se traslada la discusión del escenario académico y técnico a uno de carácter político y normativo, destacando a su vez, los desafíos a los cuales se enfrentan las autoridades al buscar evidencias en sistemas descentralizados.

En consecuencia, de los avances normativos promovidos por el Congreso de La Habana, la Convención de Budapest (Hungría), adoptada el 23 de noviembre de 2001 bajo el auspicio del Consejo de Europa, constituye el instrumento penal internacional más importantes en cuanto a los delitos informáticos. Ratificada por tres décadas, esta convención tipifica conductas como acceso ilícito a sistemas informáticos, la interceptación de datos, la interferencia en la integridad de sistemas y datos, el abuso de equipamiento informático, así como delitos transversalizados por su finalidad, como es la pornografía infantil y violaciones de la propiedad intelectual. Además, pronostica mecanismos de asistencia mutua, que facilita el intercambio de pruebas digitales y la coordinación de operaciones policiales y judiciales. Su carácter vinculante y se alcance extraterritorial han sido cruciales para establecer estándares mínimos en la persecución penal de los ciberdelitos.

Una década después, el Congreso de la ONU sobre Prevención del Delito y Justicia Penal, en su duodécima edición celebrada en la ciudad brasileña del Salvador en 2010, abordo con especial atención las amenazas cibernéticas de ámbito penal, las cuales están orientadas a la identificación de tendencias criminales emergentes y sus posibles respuestas jurídicas. En estos términos, los debates destacaron como los vacíos legales, sumados a la vetustez de las herramientas procesales, la cooperación entre naciones y la falta de figuras criminales que recojan nuevas formas de ataque a infraestructuras críticas, así como las dificultades para tipificar y sancionar patrones conductuales recientes, como los ataques de denegación de servicio y manipulación de datos en la nube (ONU, 2010, pp. 1 – 5). En este contexto, la adopción tardía de normas penales específicas posibilitó las redes criminales se consolidarán y desarrollarán técnicas de anonimato y cifrado antes de ser abordada eficazmente por la Policía y el aparato judicial.

Retomando el enfoque evolutivo del delito informático, el análisis de la ONU puso de manifiesto que, durante el periodo comprendido entre las décadas de 1960 y 1980, persistió una inquietante ausencia de legislación penal orientada a reprimir el espionaje y el sabotaje digital. Solo con la expansión masiva de Internet y la globalización del entorno digital los Estados comenzaron a reforzar sus esfuerzos para proyectar la jurisdicción penal hacia el ciberespacio, lo que a su vez generó importantes tensiones en materia de soberanía y conflictos de competencia judicial en supuestos de carácter fronterizo o transnacional (ONU, 2010, pp. 24 – 25). La lentitud de la reacción normativa abrió un margen de maniobra para que las organizaciones criminales avanzaran en el desarrollo de herramientas de cifrado y anonimato antes de que se produjera una respuesta efectiva del aparato judicial. En consecuencia, durante ese periodo, las redes ilícitas consolidaron estructuras tecnológicas progresivamente más complejas, destinadas a eludir la persecución penal.

Partiendo de estas constataciones históricas, Estados Unidos implementó una respuesta legislativa concreta mediante el CFAA de 1986, reformado en 1994. Esta legislación pionera, a nivel global, estableció un catálogo de conductas punibles relacionadas con el acceso no autorizados a sistemas informáticos para la seguridad pública y privada y sentó las bases para su penalización federal. La modificación de 1994 profundizó esta política penal a incorporar la figura del dolo eventual y la temeridad como elementos agravantes. En esta forma, las penas establecidas llegaron a contemplar hasta diez años de prisión en los casos más graves, demostrando un compromiso firme con la disuasión penal (Estrada Gavilla, s. f., p. 33). Igualmente, regulaciones estatales como la Sección 502 del Código Penal del Estado de California han impuesto limitaciones adicionales frente a delitos contra la confidencialidad, integridad y accesibilidad de los datos digitales.

En concordancia con lo expuesto respecto de la evolución normativa internacional y de las respuestas estatales frente a los delitos informáticos, resulta necesario subrayar que, durante la primera mitad de la década de 2020, se consolidó una transformación significativa en la naturaleza misma del cibercrimen. Los ciberataques pasaron de ser manifestaciones puntuales a convertirse en verdaderas estructuras de negocio, altamente especializadas y globalizadas, capaces de operar con una eficiencia cada vez mayor. Un ejemplo representativo es la expansión del *Ransomware as a Service* (RaaS), que permite a individuos con intenciones delictivas alquilar infraestructura criminal sin poseer conocimientos técnicos avanzados. Ballestero (2025) advierte que el Grupo LockBit constituye una amenaza de referencia, ya que sus operaciones han comprometido la seguridad de organismos públicos estatales de alto nivel en Europa y América Latina, evidenciando tanto una evolución técnica como una arquitectura interna de naturaleza jerárquica y logística avanzada (p. 114). En la misma línea, las agencias *European Union Agency for Network and Information Security* (ENISA), en español, Agencia de la Unión Europea para la Ciberseguridad; *la European Union Agency for Law Enforcement Cooperation* (EUROPOL), en español, Agencia de la Unión Europea para la Cooperación en la Aplicación de la Ley; y, la *Nippon Telegraph and Telephone Data* (NTT Data, 2024) coinciden en que el Phishing y los ataques DDoS continúan siendo extremadamente frecuentes, lo que demanda una actualización inmediata de las estrategias de seguridad.

1.2. La tecnoneutralidad penal como base jurídica y conceptual en la adecuación del hurto informático en el contexto latinoamericano

Durante un lapso superior a diez años, los Estados latinoamericanos y caribeños han venido consolidando sus ordenamientos punitivos con el propósito de enfrentar de manera más eficaz los delitos informáticos, los cuales han pasado a ocupar un lugar prioritario dentro de las agendas de política criminal en cada uno de sus territorios. Esta tendencia obedece a la creciente preocupación por las múltiples formas que adoptan las conductas ilícitas vinculadas al uso indebido de las tecnologías de la información y las comunicaciones (TIC), así como a la necesidad urgente de contar con instrumentos jurídicos capaces de responder a tales desafíos. En atención a este fenómeno, varios países de la región han debido revisar y actualizar sus marcos normativos, tanto desde la dimensión sustantiva como desde la procesal, procurando establecer mecanismos jurídicos específicamente

orientados a contrarrestar amenazas tecnológicas en constante evolución. En tal sentido, se vuelve indispensable analizar no solo la técnica de tipificación de estas conductas, sino también la orientación funcional que debe presidir su regulación, de manera que el Derecho Penal no se limite a describir el instrumento empleado, sino que atienda con mayor precisión a la magnitud de la afectación producida sobre los bienes jurídicos tutelados.

En este supuesto, la tecnoneutralidad normativa asume un papel central como criterio de formulación legislativa, en cuanto impide que la ley penal quede reducida a la descripción cerrada de artefactos o sistemas específicos. De ahí que la legislación no permanezca sujeta a dispositivos o sistemas específicos, sino que se exprese mediante categorías amplias, como "registros", "plataforma informática" o "acceso no consentido". Serger (2016, pp. 19 -21) subraya que esta estrategia no solo dota a la norma de mayor alcance y adaptabilidad, sino que también permite comprender fenómenos híbridos, entre ellos la defraudación electrónica o la suplantación personal por medio de las plataformas digitales, donde se articulan estructuras clásicas con medios tecnológicos.

Serger (2016, p. 21) sostiene que las legislaciones penales de los Estados deben estructurarse desde la neutralidad tecnológica, a fin de no quedar atadas a soluciones técnicas concretas que puedan volverse obsoletas en breve. Tal exigencia encuentra su fundamento en la necesidad de preservar los principios cardinales del Estado Social de Derecho y de los Derechos Humanos (DDHH). Por ello, el legislador debe evitar referencias directas a dispositivos o aplicaciones concretas, pues tales menciones comprometen la vigencia de la norma frente al cambio acelerado del entorno digital. A ello se añade que tales soluciones normativas deben corresponder a las peculiaridades del entorno digital de cada Estado, configurado por una transformación tecnológica vertiginosa y por la proyección interestatal de las conductas criminales realizadas mediante redes de datos. En esa perspectiva, la regulación de cada territorio debe evitar su dependencia de plataformas informáticas o de contextos territoriales específicos.

Uno de los ejemplos más emblemáticos de este enfoque es el Convenio de Budapest sobre ciberdelincuencia, cuya relevancia ha trascendido ampliamente el ámbito europeo. Su trascendencia se explica por la capacidad de anticiparse a los obstáculos que plantea la mutación tecnológica mediante una técnica normativa flexible, apta para comprender no solo los delitos informáticos en sentido estricto, sino también aquellas conductas cometidas mediante las TIC, en las que estos recursos funcionan como instrumentos para la ejecución de fraudes, extorsiones y otras modalidades de criminalidad digital. Como resultado, numerosos Estados de fuera de Europa, especialmente en América Latina, han seguido su modelo o han ratificado sus disposiciones.

Partiendo de lo expuesto, las notas guía elaboradas en el marco del Convenio de Budapest ofrecen criterios útiles para aplicar sus disposiciones frente a amenazas emergentes, como las redes de bots y los ataques masivos atribuidos a *ransomware, phishing* y *DDoS*. Esta función hermenéutica permite que, aun en aquellos supuestos en los que los marcos punitivos no son objeto de actualización constante, las autoridades competentes dispongan de criterios técnicos y jurídicos suficientes para interpretar de manera adecuada las manifestaciones contemporáneas de la ciberdelincuencia. Gracias a ello, incluso cuando la legislación penal o los marcos punitivos no son reformados de manera continua, las autoridades conservan herramientas técnico-jurídicas para calificar e interpretar adecuadamente las conductas emergentes. Así, sin necesidad de alterar de forma recurrente el texto original del Convenio, este preserva su vigencia operativa y su capacidad de adaptación frente a la transformación continua de las prácticas delictivas digitales.

Así pues, entre los aportes más relevantes del Convenio destaca la creación de una red transnacional de interacción permanente, conocida como la "Red 24/7", cuyo propósito es facilitar la asistencia judicial inmediata entre los Estados firmantes, especialmente en lo relativo al aseguramiento de evidencia digital. Su utilidad resulta especialmente evidente en aquellos supuestos en los que la prontitud es determinante, ya que permite preservar información almacenada en servidores ubicados fuera del territorio nacional. Por ello, constituye una alternativa mucho más eficiente que los

mecanismos tradicionales de cooperación judicial, que suelen tardar más y exigir trámites más complejos.

Aunado a lo anterior, resulta indispensable que la formulación y promulgación de políticas públicas en materia de delitos informáticos incorporen una dimensión preventiva. En tal sentido, la finalidad de la respuesta estatal no debe agotarse en la imposición de la pena, sino orientarse también a la prevención de estas conductas mediante campañas de sensibilización, programas de formación ciudadana en seguridad digital y lineamientos de buenas prácticas tanto para personas naturales como para empresas. También es importante crear protocolos de intervención, dotar de herramientas tecnológicas a los operadores jurídicos, las fiscalías y la Policía Nacional, y establecer mecanismos de evaluación que permitan medir si las estrategias están reduciendo estas conductas. De esta articulación institucional debe surgir, en consecuencia, la consolidación de unidades especializadas en delitos informáticos, concebidas conforme a criterios de eficacia y oportunidad en la respuesta estatal.

Bajo esta perspectiva, también resulta fundamental que las propuestas reformistas vayan acompañadas del personal técnico idóneo y del presupuesto suficiente para garantizar su implementación eficaz. Como advierte Serger (2016, p. 23), los países latinoamericanos deben evitar la simple reproducción mecánica, el llamado "*copy-paste*", de modelos punitivos que han resultado exitosos en otros contextos, sin atender previamente a las realidades sociales de sus propios territorios. Tal advertencia resulta especialmente pertinente en un momento en que los gobiernos de esta región todavía afrontan obstáculos para acceder efectivamente a las innovaciones informáticas vigentes en el ámbito internacional, para asegurar la debida formación de los operadores judiciales y para impulsar la investigación como vía de superación de tales asimetrías. En ese sentido, las políticas públicas deben diseñarse con un criterio de viabilidad operativa, sin renunciar por ello a una proyección transformadora.

Sin embargo, el análisis de Derecho Comparado sobre las distintas experiencias reformistas evidencia que muchas de ellas no han estado acompañadas de un verdadero fortalecimiento institucional. En varios ordenamientos, la recepción de modelos extranjeros ha generado un avance meramente formal, sin que ello se traduzca en una infraestructura institucional suficiente para enfrentar la complejidad técnica de los delitos informáticos. Ello se agrava cuando las instituciones encargadas de la persecución penal carecen de equipos técnicos especializados o de protocolos uniformes que permitan asegurar la validez de la prueba ante los jueces. En materia de ciberdelincuencia, esto resulta especialmente importante porque el éxito de una reforma depende tanto de la calidad del texto legal como de la capacidad de los órganos encargados de ejecutarlo. Una reforma aparentemente avanzada puede convertirse, en la práctica, en un mecanismo de impunidad si no logra producir decisiones válidas y ejecutables; pero también puede transformarse en un instrumento de arbitrariedad si se aplica sin límites, sin controles y sin garantías. Solo así la respuesta penal podrá ser al mismo tiempo legítima, eficaz y respetuosa de la seguridad jurídica, los derechos fundamentales y los compromisos internacionales asumidos por el Estado.

En definitiva, la evolución de los delitos informáticos exige una respuesta penal metódica, moderna y adaptable, sustentada en una visión integral que articule los avances técnicos y jurídicos indispensables para la protección efectiva de los derechos de las personas. Esta respuesta debe contemplar, asimismo, los componentes normativos y operativos asociados a la cooperación regional e internacional. En consecuencia, la adopción de una codificación técnicamente neutra, articulada con mecanismos procesales eficientes y con esquemas robustos de trabajo conjunto, posibilita la consolidación de una justicia penal apta para responder a los desafíos de la era digital.

1.3. Respuesta integral para para enfrentar los desafíos y soluciones socio - jurídicas del hurto informático en Colombia

En Colombia, una de las principales preocupaciones para las autoridades policiales y judiciales ha sido el aumento de los hurtos perpetrados por medios informáticos, problemática que cobró mayor relevancia con la promulgación de la Ley 1273 de 2009, por medio de la cual se adicionó al Código Penal el Título VII bis. A partir de esta reforma, los datos y los sistemas informáticos pasaron a integrar el ámbito de los bienes jurídicos tutelados, si bien la respuesta legislativa se circunscribió de manera apenas parcial a las exigencias de modernización que demanda esta modalidad delictiva. La doctrina ha analizado este desarrollo resaltando tanto sus aportes como sus límites. Sánchez Castillo (2017) señala que la Ley 1273 de 2009 representó un avance fundamental, pero careció de un diseño integrador apto para acompasarse con la evolución tecnológica de forma dinámica (p. 37). A su vez, la jurisprudencia ha mostrado insuficiencias, especialmente por las lagunas interpretativas que persisten en torno al hurto por medios informáticos y su delimitación frente a figuras próximas, como la estafa informática o la transferencia no autorizada de activos.

De igual manera, las publicaciones académicas recientes han señalado que en Colombia persiste una fragilidad institucional significativa para la persecución eficaz de los delitos informáticos. Bolívar Londoño y Carvajal Ríos (2024) advierten que la legislación especial en vigor no ha remediado las carencias en la formación técnica del aparato judicial, ni su enlace con bases de datos, ni los mecanismos de colaboración internacional. Esta insuficiencia se ve reforzada por la complejidad probatoria inherente a tales conductas, en la medida en que la huella digital suele carecer de permanencia o puede ser trasladada con relativa facilidad. Por ello, Herrera Peralta, López Ordóñez y Rey Durán (2018) han sostenido que la mera existencia de un tipo penal no es suficiente para asegurar una respuesta eficaz, en tanto los obstáculos tecnológicos y procedimentales restringen, siquiera parcialmente, la judicialización de los presuntos autores (p. 24).

Asimismo, los estudios de Armijo Catalán, Bouillet Carroza y Delere (2025), junto con los datos presentados por Gutiérrez (2025), evidencian un incremento progresivo de los incidentes vinculados con esta modalidad punitiva. Sin embargo, la persistente invisibilización de tales hechos distorsiona la percepción de su real dimensión. En este orden, Parra (2024) evidencia, mediante una investigación realizada en un departamento colombiano, que numerosos ciudadanos desconocen los canales de denuncia o desconfían de la eficacia de la administración de justicia (p. 19). Esta percepción social no solo favorece la impunidad, sino que también retrasa la construcción de políticas públicas capaces de enfrentar con seriedad este fenómeno. A ello se suma lo advertido por Carrizosa Acosta (2024), quien señala que la creación de identidades falsas, el uso de redes cifradas y otras herramientas de ocultación dificulta de forma intensa la investigación, sobre todo cuando tales dinámicas se articulan con actores privados del entorno digital (p. 66).

Por otro lado, en el plano jurisprudencial, Martínez–Vélez desarrolla un análisis de decisiones recientes en las que se problematiza si el hurto informático encuentra una mejor subsunción típica dentro de la figura de la estafa digital. A partir de las sentencias analizadas por este autor, se advierte una línea jurisprudencial que tiende a encuadrar estos supuestos en figuras penales clásicas, lo cual pone en evidencia una posible falta de capacitación judicial o un rezago jurisprudencial en la interpretación de conductas penales adaptadas al entorno digital (p. 44). En concordancia con ello, Gómez Pineda, Gómez Orozco y Vidal Flórez (2023) advierten que la inexistencia de una política criminal estructurada y especializada para la persecución de este delito ha derivado en respuestas penales “a medias”, donde la prevención se reduce a un simple “paño de agua tibia” y el componente represivo no alcanza una formulación consistente (p. 71). En el mismo sentido, Navarro Ramírez y Díaz Serrano (2024) cuestionan la escasa articulación entre las competencias de los jueces penales municipales y la complejidad tecnológica que exigen este tipo de conductas, lo que revela una tensión persistente entre diseño institucional y realidad delictiva.

Desde una perspectiva criminológica, López Avilés (2014) y Serrano Buitrago muestran que el hurto informático ha pasado de ataques simples de *phishing* a estrategias más complejas, como la ingeniería social, el *ransomware* y la manipulación de información financiera. En el caso colombiano, esta conducta ya no se restringe al ámbito interno, puesto que los atacantes pueden operar desde otras jurisdicciones y aprovechar vulnerabilidades locales. En concordancia con ello, Gamba Velandia (2019) afirma que la transferencia no legítima de activos es una de las conductas más recurrentes y, a la vez, menos perseguidas, debido sobre todo a la insuficiente capacidad de gestión de la forensia digital durante las primeras fases de la investigación penal (p. 5).

En suma, el hurto por medios informáticos en Colombia exige una revisión integral, tanto sustantiva como procesal, por tratarse de un fenómeno de gran magnitud. El incremento de las denuncias, junto con el análisis de las decisiones judiciales y la velocidad de transformación del mundo digital, configura un escenario de retos permanentes para la administración de justicia. En tal sentido, la Ley 1273 de 2009, más que significar una culminación, constituyó apenas el umbral de un proceso que entre 2022 y 2025 debe valorarse en sus dimensiones operativa, jurisprudencial, técnica y social. En esa dirección, Pena Peña (2023) destaca que un verdadero cambio institucional permite articular la actualización legislativa, la formación continua, la cooperación internacional y la sensibilización ciudadana (p. 79). De este modo, el énfasis de la política criminal no debe situarse únicamente en la sanción, sino también en la prevención y en la restauración de derechos frente a las nuevas formas de cibercrimen.

Capítulo 2. El estándar probatorio en el hurto por medios informáticos, y la articulación entre jurisprudencia y doctrina

Esta sección retoma y desarrolla de forma más detenida la tensión previamente esbozada entre, por un lado, la configuración normativa contenida en la Ley 1273 de 2009, complementada por las disposiciones procesales de la Ley 1928 de 2018, y, por otro, la realidad operativa que han mostrado las instituciones colombianas durante el periodo entre 2022 y 2025. En el plano formal, el derecho sustantivo construye una estructura técnica aparentemente robusta, integrada por figuras como el acceso abusivo, el hurto informático y los agravantes por afectación de infraestructuras estratégicas, además de mecanismos procesales para la obtención de prueba digital y la cooperación judicial. No obstante, el contraste con la praxis reciente pone de manifiesto una fisura estructural en donde la normativa opera más como horizonte programático que como conjunto de reglas dotadas de eficacia sistemática. Esta distancia no deriva exclusivamente de carencias presupuestarias, ciertamente existentes, sino también de una desarticulación técnico-procesal. En efecto, los altos estándares probatorios exigidos por la jurisprudencia, sumados a la disparidad institucional en materia de peritaje y cadena de custodia, terminan por neutralizar, paradójicamente, la persecución penal que la propia normativa procura impulsar.

Así, la función preventiva atribuible a la Ley 1273 de 2009 muestra, a la luz de los hechos, una dualidad compleja. Aunque el marco normativo incorpora instrumentos disuasorios como son los agravantes, las medidas cautelares específicas y la valoración de la peligrosidad tecnológica, a medida que, la prevención real exige algo más que la simple tipificación de conductas. Por tales razones, se requiere, en particular, estructuras complementarias, como registros públicos de resultados, campañas sostenidas de ciberhigiene, obligaciones de notificación para las entidades privadas y un sistema de indicadores que permita relacionar la inversión estatal con la disminución de incidentes. Sin embargo, entre 2022 y 2025 predominó una prevención dispersa, basada en acciones aisladas y no en una política nacional coherente. En definitiva, la ausencia de datos homogéneos, junto con la inexistencia de indicadores procesales como el tiempo de resolución o la tasa de conversión de denuncias en condenas, hace que toda apreciación sobre su eficacia permanezca condicionada por la provisionalidad.

En materia de persecución penal y valoración probatoria, la doctrina judicial reciente ha configurado una dinámica ambivalente. Mientras la Sala de Casación Penal de la CSJ y la Corte Constitucional han reforzado los controles de transparencia y constitucionalidad sobre la prueba digital, ese avance ha venido acompañado de efectos colaterales problemáticos. Ya que, la exigencia de narrativas precisas sobre los accesos, de secuencias cronológicas verificables mediante *hashes* y de peritajes reproducibles contribuye a preservar las garantías procesales y a conferir legitimidad a las decisiones judiciales. Sin embargo, el aumento de esos estándares desplaza la presión hacia una infraestructura técnica que no existe de manera uniforme en Colombia. Empero, al elevar tales exigencias, también desplaza el peso de su cumplimiento hacia recursos materiales e institucionales cuya distribución en el territorio nacional es desigual, como laboratorios acreditados, formación especializada y sistemas de certificación. De ahí que, frente al contraste entre un mayor rigor judicial y las limitaciones estructurales del Estado, exista el riesgo de que procesos sustentados en indicios robustos concluyan en absoluciones por vicios formales, convirtiendo así el formalismo exigido en un mecanismo indirecto de impunidad técnica.

La Sentencia SP592-2022 de la CSJ, conforme a la lectura crítica de Madariaga, descansa sobre la premisa de elevar el estándar probatorio técnico en la persecución de los delitos informáticos. Ese criterio robustece la seguridad jurídica y las garantías procesales, pero también genera una tensión práctica innegable. Tal orientación contribuye a consolidar el sistema de garantías y a fortalecer la seguridad jurídica; sin embargo, produce una tensión práctica de no poca relevancia. En ausencia de capacidades forenses adecuadas y de una infraestructura institucional robusta, la exigencia de peritajes reproducibles, cadena de custodia digital y registros de conexión verificables puede conducir

a insuficiencia probatoria y, por ende, a absoluciones aun en presencia de indicios relevantes. Madariaga insiste, además, en que la CSJ no transforma el tipo penal en uno que exija probar el lucro como regla general; lo que demanda es que la finalidad, cuando resulte relevante para la calificación o para su conexión con otros ilícitos, conste de manera expresa en la narración fáctica y en los medios probatorios. En suma, la providencia y su recepción doctrinal plantean dos exigencias paralelas: mayor rigor metodológico en la producción de evidencia digital y la adopción de políticas y medidas administrativas concretas, como formación especializada, inversión y protocolos técnicos, que hagan viable la aplicación de ese nuevo estándar (Corte Suprema de Justicia, 2022, pp. 6–11; Madariaga, 2022).

Las repercusiones prácticas entre 2022 y 2025 se derivan directamente en la articulación entre la jurisprudencia y la doctrina: La Sentencia SP592- 2022 fija criterios homogéneos de valoración que orientan la persecución del hurto por medios informáticos, pero la eficacia de esos criterios dependerá de la capacidad institucional para generar pruebas digitales que cumplan los requisitos forenses exigidos por la Sala de Casación Penal de la CSJ (Corte Suprema de Justicia, 2022, pp. 10 – 16). Como apunta Madariaga, la providencia supone un avance interpretativo que protege garantías procesales, no obstante, sin la profesionalización de la pericia informática y sin mecanismos de cooperación público – privada para la preservación de la evidencia, al aumento del estándar técnico puede terminar facilitando la impunidad técnica (Madariaga, 2022). Por tanto, al incluir la Sentencia SP592-2022 en el capítulo es recomendable presentar sentencia y doctrina como una unidad analítica: La Jurisprudencia delimita el qué probatorio, la doctrina indica el cómo operacionalizarlo; y ambas proponen medidas concretas, protocolos de cadena de custodia digital, criterios periciales mínimos, laboratorios forenses y formación continua, esenciales para que la exigencia jurisprudencial no reduzca la eficacia persecutoria (Corte Suprema de Justicia, 2022, pp. 6 – 16; Madariaga, 2022).

2.1. La evolución jurídica global frente al hurto informático y los mecanismos internacionales de prevención y sanción

Los vacíos jurídicos relacionados con el hurto cometido mediante herramientas informáticas comenzaron a evidenciarse desde los primeros informes elaborados por la OCDE en 1983, en torno al fraude electrónico. Desde ese momento, se recomendó a los Estados la incorporación de tipos penales aptos para atender las particularidades del entorno tecnológico. De ese modo, las naciones fueron llamadas a incorporar en sus normativas penales disposiciones que se adecuaran a las exigencias propias de un medio digital en continua transformación. Estas orientaciones tuvieron una incidencia considerable, pues dejaron al descubierto la insuficiencia de los marcos tradicionales y la necesidad de emprender una reforma legislativa que conciliara las exigencias internacionales con los estándares técnicos entonces reconocidos, en un contexto de cambio tecnológico continuo (Candelario Samper & Rodríguez Bolaños, 2015, p. 140).

Ante el crecimiento de la comisión de los delitos informáticos, obviamente, el impacto de la tecnología en dichas malas prácticas, la OCDE invitó a los Estados firmantes a la formulación de una política criminal, la cual combata dichos delitos. En consecuencia, su adecuación legislativa posterior se debió estructurar un proceso de reforma penal con la capacidad de unificar los estándares internacionales con los contextos locales. En esta medida, Amaya-Cristancho y Cortés Vargas sostienen como el hurto de datos personales exige unos protocolos técnicos para la interpretación de bitácoras (“*logs*”) y metadatos, para lo cual, estos autores proponen la creación de unidades especializadas de delitos informáticos y la implementación de una cadena de custodia de evidencias digitales (Amaya-Cristancho & Cortés Vargas, 2011, pp. 180–181). Pues, tales medidas jurídicas permiten una reconstrucción veraz del *modus operandi* de los ciberdelincuentes, por tal razón, las instituciones han hecho un mejoramiento exponencial de la efectividad de la imputación penal, lo cual significa que se ha presentado una reducción significativa de la impunidad en delitos técnicamente elaborados.

En este contexto, el reconocimiento de la validez probatoria de la evidencia electrónica se ha proyectado en múltiples sistemas jurídicos y ha quedado reflejado en diversos estándares internacionales. Así, en el Reino Unido se promulgó en 1984 la *Police and Criminal Evidence Act* y, posteriormente, en 2015, las *Criminal Practice Directions,* en las que se establecen directrices precisas sobre la obtención y custodia de información informática. En Australia, la Evidence Act de 1995 excluyó los registros computacionales de la Regla de *Hearsay* siempre que estén acompañados de certificaciones técnicas. En India, por su parte, el *Information Technology Act* incorporó dos disposiciones específicamente destinadas a establecer requisitos equivalentes de certificación (Contreras – Manrique et al, 2004, pp. 107 – 109).

Igualmente, en 1990, durante el *Octavo Congreso de la ONU sobre Prevención del Delito y Tratamiento del Delincuente*, celebrado en La Habana, la ONU exhortó a los Estados signatarios a implementar programas permanentes de capacitación dirigidos a jueces, fiscales y cuerpos de policía en materia de criminalidad informática (ONU, 1990). En desarrollo de dicha orientación, los distintos miembros impulsaron convenios interinstitucionales encaminados a la elaboración de manuales, cursos y diplomados especializados en el análisis de los delitos cometidos mediante medios informáticos. Estas acciones permitieron conformar equipos de expertos en diversas disciplinas y, con ello, enfrentar de manera más sólida el hurto informático.

Una década más tarde, hacia el año 2001, en Budapest (Hungría) se firma el Convenio sobre Ciberdelincuencia, el cual se convierte en el primer tratado internacional orientado a combatir el ciberdelito, en el cual se determinaron las bases para la tipificación penal, los mecanismos de cooperación internacional, y las técnicas de investigación digital. Su novedad radicaba en la posibilidad que brindo para la adhesión de países no europeos, ante lo cual alcanzaron más de cincuenta ratificaciones. Este tratado está estructurado en cuatro bloques como son en primera medida, el acceso e interceptación ilícita o ataques informáticos; en segundo término, se puede encontrar los delitos informáticos propiamente dichos como son el fraude y la falsificación digital; están aquellos vinculados directamente con los contenidos ilícitos, específicamente la pornografía infantil en sus distintas maneras de reproducción, distribución o posesión; y todo lo relativo con los derechos de propiedad intelectual, como la piratería digital. Incluso en este mismo instrumento existen disposiciones comunes como es la tentativa, complicidad, responsabilidad penal de personas jurídicas y reglas rectoras sobre las penas, donde se hace determinante que las mismas sean efectivas, proporcionales y disuasorias, eso sí, respetando la soberanía punitiva de cada Estado Parte (Herdler, 2024, pp. 3 -4).

A lo anterior puede añadirse que las propuestas de cooperación internacional han influido de manera significativa en la persecución de los delitos informáticos. Así lo evidencia la *Resolución A/CONF.213/L.6/Rev.2 del 12.º Congreso de la ONU sobre Prevención del Delito (2010),* en la cual se definieron diversos mecanismos de asistencia mutua para la obtención de pruebas electrónicas, así como criterios orientados a la armonización de los procedimientos de intercambio de información entre Estados, conforme a lo dispuesto en su Artículo 22. En consecuencia, los distintos Estados Parte que se han adherido a dicho instrumento han logrado optimizar la práctica probatoria en otros territorios y elevar la eficacia de la investigación de conductas informáticas de proyección transnacional. Estas acciones permitieron conformar equipos de expertos en diversas disciplinas y, con ello, enfrentar de manera más sólida el hurto informático.

Con ocasión de este mismo instrumento internacional, en distintas partes del mundo surgieron propuestas dirigidas a incorporar como agravantes los ataques perpetrados contra infraestructuras críticas, así como a establecer sanciones más rigurosas para los ataques masivos. La finalidad de estas reformas fue reforzar las sanciones penales aplicables a este tipo de infracciones y regular la producción y comercialización de herramientas de *hacking*, en un escenario transformado por la proliferación de la Inteligencia Artificial (IA). Estas tendencias se alinean con los requerimientos suscritos por la Unión Europea y los Estados Unidos a través de sus marcos de referencia, entre ellos la NIS2 y la *Infrastructure Protection Act*. A su vez, Canadá y Australia han previsto en su legislación penal delitos vinculados con el uso de DDoS y *botnets*. Por ello, en la región se consolida la exigencia de certificaciones obligatorias para infraestructuras críticas y la promoción de APP's como mecanismo de gestión responsable de vulnerabilidades (ONU, 2010, pp. 15–19).

Ahora bien, al abordar las categorías de *phishing* y *skimming*, Estrada Posada y Somellera (1998) identifican una relación directa entre determinados marcos normativos de los Estados Unidos, en particular la *Computer Fraud and Abuse Act* (CFAA), que tipifica el *phishing* como delito federal, y la *Payment Card Industry Data Security Standard* (PCI DSS), o Estándar de Seguridad de Datos para la Industria de Tarjetas de Pago, cuya incidencia ha fortalecido los mecanismos de control antiskimming en los puntos de venta. En el ámbito de la Unión Europea (UE), la *Directiva 2013/40* sobre ataques a los sistemas de información introduce agravantes vinculados al uso fraudulento de datos personales, mientras que el Reglamento General de Protección de Datos (RGPD) intensifica tanto el régimen sancionatorio como las obligaciones de información. En contraste, la Convención de Budapest y las iniciativas promovidas por la OCDE persiguen la armonización de conceptos y el fortalecimiento de la cooperación internacional frente a estas formas de criminalidad informática.

Por último, el *Informe A/79/460* de la ONU (2024) destaca el crecimiento exponencial de las maneras como los ciberdelincuentes cometen sus acciones punibles mediante el empleo de las TIC's como es el uso de *malware* sofisticado hasta la programación de redes de *bots*, para llevar a cabo fraudes, extorsiones y ataques contra sistemas de información estratégicos, ante lo cual, se debe hacer una perentoria revisión de la normatividad nacional y los instrumentos internacionales. Así mismo, pone un especial énfasis e insiste en la necesidad de capacitar a los operadores judiciales en conocimientos acerca de la forensia digital, y, equiparlos de un *hardware* y *software* garantes de la cadena de custodia de la evidencia. Simultáneamente, invita a los Estados Firmantes al fortalecimiento de la cooperación interestatal por medio de acuerdos de asistencia judicial y policial, como así mismo, la creación de plataformas de intercambios de conocimiento que le den agilidad a la obtención de evidencias digitales. Igualmente, promueve el establecimiento de APP´s direccionadas a la prevención y anticiparse a las consecuencias surgidas desde cuando se cometen las ciberamenazas por parte de los perpetradores, ante lo cual, simultáneamente se plantea la urgencia de determinar la necesidad de estandarizar protocolos que refuercen la seguridad de los sistemas esenciales.

2.2. Impulsando la ciberjusticia a través de la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) en el escenario latinoamericano

En el ámbito latinoamericano, la OEA y el BID han desempeñado una función cardinal en la estructuración de una agenda común orientada a la persecución y tratamiento de los delitos informáticos, en particular en lo atinente a la adopción de los principios contenidos en el Convenio de Budapest. Esta labor no ha operado de forma abstracta, sino mediante foros multilaterales de coordinación, como la Reunión de Ministros de Justicia o de Ministros o Procuradores de las Américas (REMJA), desde los cuales se ha buscado, por más de veinte años, acercar los sistemas jurídicos de los Estados Miembro, promover la circulación de experiencias exitosas y robustecer los mecanismos de cooperación jurídica internacional. De forma complementaria, el Grupo de Trabajo en Delito Cibernético de la OEA, creado en 2004, ha recomendado a los Estados Miembros ajustar tanto sus reglas sustantivas como sus procedimientos a los parámetros del Convenio, con el fin de

ofrecer respuestas normativas más coherentes frente a la criminalidad digital (OEA & BID, 2016, pp. 19–23).

Así fue, como en el año 2006 se realiza la VI REMJA, efectuada en República Dominicana, cuya reunión parlamentaria se constituye en un hito importante en América Latina y el Caribe. Por ello, a partir de dicho evento, diferentes naciones iniciaron expresamente el proceso de adhesión al Convenio de Budapest, impulsados no solo por los mandatos legales, sino además por la necesidad de consolidar las estructuras organizativas frente a los avances tecnológicos. Ante esto, los primeros estados en adherirse al Convenio sobre la Ciberdelincuencia fueron Costa Rica y México, y más tarde se sumaron los gobiernos de Argentina, Chile, Colombia, Panamá, República Dominicana, Paraguay y Perú (Serger, 2016, pp. 21–22). De esta manera, la OEA reitera en las recomendaciones de articular las legislaciones nacionales con las directrices internacionales (BID & OEA, 2020, pp. 26 - 28).

Por lo tanto, el acompañamiento de la OEA y de la BID han contenido iniciativas concretas como son la realización de talleres técnicos para jueces, fiscales y policías; elaboración de ejercicios interpretativos; y el desarrollo de redes de cooperación interestatal. Entre estas propuestas se destaca una red de contacto permanente "24 / 7" donde se permite dar una respuesta inmediata a casos internacionales (OEA & Trend Micro, 2013). Tales propuestas han consolidado la capacidad de respuesta como las estrategias de prevención de los Estados frente al ciberdelito, impulsando una cultura de ciberresiliencia en la región. De esta forma, la OEA ha aportado en forma destacada a la reforma de las legislaciones penales y procesales, fomentando el establecimiento de unas figuras en particular y funciones procesales idóneas para la obtención de pruebas electrónicas.

Desde otra línea de análisis, la presión política y técnica ejercida por la OEA se ha transformado en el punto de inflexión para poderse realizar esta "ola reformista" en varias naciones latinoamericanas; lo cual ha demostrado como esta adecuación a la normativa adecuación a partir de los estándares internacionales lo cual puede potencializar la modernización institucional frente al tema de la ciberdelincuencia. En este escenario, han sido bien aceptadas las propuestas de formación técnica para los operadores jurídicos lo cual ha complementado la elaboración de manuales donde se interpreten dichas disposiciones y el establecimiento de permanentes redes operativas. Tales disposiciones han contribuido a la visibilización de la lucha contra el cibercrimen como una prioridad estratégica y simbólica en las agendas gubernamentales. Por tales razones, la progresiva adopción del Convenio de Budapest La adopción gradual del Convenio de Budapest en Latinoamérica ha servido como una excelente estrategia para consolidar los sistemas penales, y así asegurar la colaboración interestatal en medio de un ecosistema penal donde el delito informático traspasa fronteras (Serger, 2016, pp. 21–22). Surgiendo de esta forma un modelo de justicia penal donde se articulan la capacidad de ajuste institucional, la cooperación internacional y la modernización tecnológica, sin dejar de lado la protección de los Derechos Fundamentales.

2.3. La Ley 1273 de 2009, la Ley 1928 de 2018 y la jurisprudencia clave. Retos probatorios y cooperación internacional en el hurto por medios informáticos en Colombia

A lo largo de la última década, el hurto realizado mediante recursos informáticos se ha convertido en un problema central para el sistema penal colombiano, dada la rápida transformación de sus modalidades y el incremento de la capacidad técnica de los delincuentes que se aprovechan de las falencias tecnológicas. En ese contexto, la Ley 1273 de 2009 representó un avance normativo significativo, al incorporar al ordenamiento penal tipos como el acceso abusivo a un sistema informático, la interceptación de datos y la alteración de sistemas, así como mecanismos procesales y herramientas de investigación forense digital. Sin embargo, la implementación de esta normatividad ha evidenciado serias limitaciones estructurales, entre ellas la falta de estándares nacionales claros para la cadena de custodia electrónica, la insuficiente formación y acreditación de expertos, y la ausencia de protocolos efectivos de coordinación interinstitucional.

Un examen riguroso de la Ley 1273 de 2009 permite sostener que esta constituyó un punto de inflexión en el Derecho Penal colombiano, al incorporar al ordenamiento un régimen específico para la tutela de la información y de los datos frente a las nuevas modalidades de criminalidad informática. A través de ella se consagraron figuras como el acceso abusivo a un sistema informático y la violación de datos personales (Artículo 269F, Código Penal), destinadas a reprimir tanto la intromisión no autorizada en sistemas de información como la apropiación o utilización ilegítima de datos electrónicos. De igual forma, estableció una agravante para los eventos en que el ataque compromete infraestructuras esenciales, como las redes de comunicación o los sistemas de salud, lo cual responde a la necesidad de salvaguardar bienes jurídicos de alta sensibilidad en una sociedad progresivamente digitalizada.

En el ámbito procesal, la normatividad punitiva legitimó el uso de peritajes informáticos y de elementos probatorios destinados a demostrar los hechos tanto para la acusación como para la defensa, además de autorizar la interceptación judicial de comunicaciones y la preservación de registros digitales bajo una custodia estricta. No obstante, la inexistencia de una reglamentación secundaria suficiente, unida a la ausencia de protocolos técnicos estandarizados, ha generado decisiones judiciales divergentes y retrasos que comprometen la integridad de la cadena de custodia. En igual sentido, el componente preventivo de la Ley ha visto reducida su eficacia por la ausencia de instrumentos concretos capaces de fortalecer una cultura de ciberseguridad ciudadana y de protección digital en el ámbito estatal y empresarial.

Ahora bien, siguiendo la misma línea de argumentación se tiene que la Ley 1928 de 2018 constituyó un paso relevante en la regulación de los delitos informáticos, al reconocer expresamente a la evidencia digital y adaptar el procedimiento penal a las exigencias propias de la tecnología. La disposición determina que los registros electrónicos, tales como *logs* de acceso, comunicaciones digitales y rastros informáticos; poseen la misma fuerza probatoria que los documentos físicos, siempre que se cumpla con la autenticidad y la cadena de custodia (Ley 1928 de 2018, Artículos 1 - 3). Por tales razones, desde su implementación la FGN incremento en un veinticinco por ciento la práctica de peritajes forenses en delitos electrónicos, reforzando la etapa de instrucción (Cortina Vidal & Puentes Mora, 2018, pp. 45 – 49).

Además, la normativa incorporó los mecanismos especiales para obtener información almacenada en sistemas digitales, exigiendo una resolución judicial motivada para las interceptaciones electrónicas y para la extracción copia o copia de datos de servidores (Ley 1928 de 2018, Artículo 5).Sin embargo, la carencia de plazos máximos definidos para resolver tales solicitudes puede dilatar la fase de indagación y poner en peligro la integridad de evidencia digital, circunstancia que provoca dudas en los operadores judiciales y los sujetos procesales (Navarro Ramírez & Díaz Serrato, 2024, pp. 22 - 26).

En materia de garantías procesales, la norma obliga a que las actuaciones intrusivas; por ejemplo, las interceptaciones; guarden proporcionalidad, estén debidamente motivadas en términos objetivos y quedan sujetas a control judicial posterior del Juez de Garantías (Ley 1928 de 2018, Artículo 6). Sin embargo, en la práctica se han registrado peticiones amplias de “acceso total” a sistemas, sin parámetros claros sobre su extensión temporal o material, lo que ha generado objeciones constitucionales. Finalmente, aunque el Consejo Superior de la Judicatura cuenta con la potestad para formular planes en formación de ciberdelincuencia aún demanda reforzamiento para garantizar la aplicación uniforme de los protocolos en todo el país (Jiménez & Manjarrés, 2012, pp. 75 – 78; Parra. 2024).

Al siguiente año, la Corte Constitucional en la Sentencia C – 224 de 2019, decretó la exequibilidad de la Ley 1928 de 2018 mediante la cual se aprobaba el Convenio sobre la delincuencia (Budapest, 2001), pero lo hizo acompañada de una motivación robusta que define límites y obligación para su aplicación interna. El Alto Tribunal sostuvo que el propósito del Convenio de la Ley aprobatoria es intensificar la colaboración internacional para investigar y perseguir delitos informáticos, objetivo compatible con la Constitución de 1991 siempre y cuando su implementación respete garantías fundamentales: Privacidad, *Habeas Data*, Debido Proceso; y al Principio de Soberanía Penal. Por tanto, la Corte Constitucional (2019) avaló la adhesión, pero la condicionó a salvaguardas constitucionales que eviten prácticas arbitrarias en la obtención y la transmisión de datos. De esta forma, la adhesión no habilita acciones extrajudiciales ni sustituye los controles locales: Todos los procedimientos y solicitudes de cooperación deberán pasar por el control judicial y ajustarse a los Principios de Necesidad y de Proporcionalidad.

Por tales razones, la Corte Constitucional (2019, pp. 45 – 46) enfatizó dos categorías de limitación que afectan de manera directa en la puesta en práctica en la implementación de investigaciones sobre hurto cometido a través de medios informáticos: **(i)** El establecimiento de controles judiciales y procesales específicos que regulen la intervención en comunicaciones y el acceso a datos personales, con el propósito de garantizar la intimidad, y; **(ii)** la preservación estricta de la cadena de custodia y la aplicación de estándares probatorios propios de la evidencia digital, acompañados de protocolos técnicos que preserven de la validez de la prueba. El Fallo reconoció la tensión entre la Cooperación Internacional, necesaria por la dispersión geográfica de servidores y operadores; esta debe realizarse conforme a la Constitución y a la legislación interna. El mismo fallo también llamó a una colaboración activa de autoridades, entes privados y centros académicos en desarrollo de protocolos y prácticas que fortalezcan el respeto de los derechos fundamentales.

Las implicaciones derivadas del tratamiento jurídico del hurto a través del hurto informático presentan una doble vertiente: Inicialmente, la declaración de exequibilidad fortalece el soporte internacional y posibilita una asistencia recíproca más eficaz en la investigación de conductas que superan las fronteras; y, en segunda instancia, consiste en la imposición de un umbral constitucional que exige robustecer las capacidades institucionales mediante la creación de unidades especializadas, la certificación de peritos forenses y la adopción de protocolos para el manejo y transporte de evidencias digitales (Corte Constitucional, 2019, pp. 47 – 48). En el plano operativo, esta decisión se traduce, como preciso el Tribunal, en la obligación de que el acceso de datos y las interceptaciones se realicen únicamente mediante procedimientos judicializados, además de requerir un marco normativo y una capacitación adecuada para que jueces, fiscales y cuerpos policiales puedan evaluar técnicamente las pruebas digitales. En definitiva, la providencia no solo valido la compatibilidad del Convenio de Budapest con la Constitución Política, sino que delineó los principios que condicionan su implementación efectiva.

Mientras tanto, la Sala de Casación Penal de la CSJ, en la Sentencia SP-92 de 2022, efectuó una descomposición minuciosa del tipo penal de acceso abusivo, al identificar sus verbos rectores como son “acceder” y “mantenerse”, la ausencia o el exceso de autorización, la modalidad dolosa y la distinción entre *insider* y *outsider*; sobre esa base, construyó un mapa probatorio que exige a la FGN describir con precisión la intervención efectiva en el Sistema Penal Colombiano (Corte Suprema de Justicia, 2022, pp. 2 -6). En criterio de Madariaga (2022), esta labor cumple una función pedagógica y normativa, pues la providencia no se restringe a reiterar el texto legal, sino que traduce sus elementos en exigencias operativas, al demandar que la narrativa fáctica y la prueba técnica conecten el acceso informático con la falta de autorización y con la modalidad ilícita relevante. Esta integración doctrinal y jurisprudencial busca evitar decisiones fundadas en conjeturas y orienta a los operadores judiciales hacia el uso de evidencia técnica verificable (CSJ, 2022, pp. 6 – 9; Madariaga, 2022).

La *Ratio Decidend*i de la Sentencia SP592-2022, en consonancia con la lectura propuesta por Madariaga, reside en la elevación del estándar probatorio técnico, decisión que robustece la seguridad jurídica y las garantías procesales, pero que también deja al descubierto una tensión de ejecución: cuando no existe infraestructura forense idónea, la exigencia de peritajes reproducibles, cadena de custodia digital y registros verificables puede traducirse en un déficit probatorio capaz de conducir a absoluciones aun en presencia de indicios de entidad significativa (CSJ, 2011, pp. 6 – 11; Madariaga, 2022). El punto fino que Madariaga destaca es decisivo: la CSJ no ha convertido esta figura en una modalidad que imponga, por regla general, acreditar el lucro; la obligación surge únicamente cuando la finalidad resulta determinante para la calificación jurídica o para vincular otros delitos, supuesto en el cual debe aparecer demostrada en la acusación y en la prueba. Bajo esa lógica, la convergencia con buenas prácticas internacionales es clara: no basta con elevar el estándar; es indispensable dotarlo de soporte material mediante capacitación especializada, laboratorios forenses robustos y protocolos verificables, de modo que la dogmática probatoria no se disocie de la capacidad institucional para ejecutarla (CSJ, 2022, pp. 9 – 14; Madariaga, 2022).

Por esto mismo, las consecuencias operativas entre 2022 y 2025 derivan directamente de esta articulación jurisprudencia – doctrina: Sentencia SP592- 2022 establece criterios uniformes de valoración que orientan la persecución del hurto por medios informáticos, pero su efectividad real estará condicionada por la capacidad institucional para producir pruebas digitales conformes a los requisitos forenses de la Sala exige (Corte Suprema de Justicia, 2022, pp. 10 -16). De esta manera, es como Madariaga resume que la providencia constituye un avance interpretativo que salvaguarda el debido proceso; no obstante, en ausencia de peritos especializados y de mecanismos público – privados eficaces para la preservación de indicios, el estándar técnico podría terminar incrementando la impunidad técnica.

Capítulo 3. Política criminal y prácticas investigativas frente al hurto por medios electrónicos un balance comparado entre modelos regionales y la experiencia colombiana

Este capítulo se estructura sobre la premisa de que la Ley 1273 de 2009 constituyó, en su momento, una respuesta normativa temprana y conceptualmente sólida, en la medida en que incorporó un bloque destinado a la tutela de la información y de los datos. No obstante, su balance entre 2022 y 2025 exige un examen situado, atento no sólo a su texto, sino también a sus efectos sociales e institucionales: la pregunta decisiva es si, en la práctica, sus disposiciones han generado prevención real, investigaciones consistentes y una capacidad disuasiva verificable frente al hurto informático. La discusión se organiza en dos dimensiones complementarias. El segundo examina la aptitud institucional para transformar una denuncia en imputación y, posteriormente, en una cadena probatoria legítima, mediante peritaje, cadena de custodia y cooperación nacional e internacional. En la distancia entre la previsión normativa y su realización procesal se inserta el propósito del capítulo, en donde se realiza una aproximación crítica y comparada sobre la eficiencia de las herramientas jurídico-procesales de la Ley 1273 de 2009 entre 2022 y 2025, integrando estadísticas de denuncias, criterios jurisprudenciales y prácticas institucionales para detectar cuellos de botella y proponer ajustes en política criminal y técnica. A esa discusión se incorpora la reevaluación de las lecciones de Argentina, Brasil, Chile, Estados Unidos y México, ahora colocadas frente a la evidencia empírica colombiana reciente y a los desarrollos jurisprudenciales que han ido modulando la interpretación de los tipos introducidos por dicha ley.

Examinando la evidencia cuantitativa, el panorama en Colombia resulta ambivalente y obliga a relativizar lecturas optimistas: Tanto fuentes oficiales como privadas agregan cifras considerables de denuncias de delitos informáticos donde la Policía Nacional consignó sesenta y cinco mil setecientos noventa y cuatro (65.794) denuncias entre 2022; y cincuenta y nueve mil treinta y tres (59.033) en 2023, lo que evidencia fluctuaciones que pueden deberse tanto a cambios reales en la incidencia como a variaciones en la forma de denunciar; además, en 2024 algunas fuentes reportaron un fuerte incremento, por ejemplo, setenta y siete mil ochocientos sesenta y seis (77.866) denuncias, lo que pone de relieve la volatibilidad del fenómeno y la necesidad de prudencia al mirar tendencias cortas. En suma, esas magnitudes indican que la demanda de respuesta institucional es elevada y creciente, y subrayan que tipificar no es suficiente: Sin una cadena de valor institucional: Formación continua, laboratorios forenses adecuados, convenios con proveedores y bases de datos coherentes; la tasa de resolución será baja y la prevención quedará limitada.

Observando la evolución jurisprudencial y doctrinal, el avance más importante en el lapso analizado ha sido la paulatina concreción de los elementos normativos del acceso abusivo y de las conductas conexas de la Ley 1723 de 2009. Por ello, la Corte Constitucional y la doctrina especializada han ido delimitando mejor los verbos que caracterizan la conducta, los objetos materiales o lógicos como son los datos y sistemas, y los márgenes de imputación, lo que ayuda a prever las consecuencias penales. Aún así, esas precisiones no siempre llegan por igual a la practica investigativa ni a la formación de quienes aplican la ley. Pronunciamientos recientes han enfatizado en la necesidad de valorar la prueba tomando en cuenta la fugacidad y replicabilidad de la evidencia digital y han identificado vacíos técnicos como son las dificultades en la preservación de pruebas entre países y el manejo procesal de criptomonedas que dificultan el éxito probatorio en hurtos por medios electrónicos. Si la jurisprudencia consolida estándares claros sobre intención, acceso y daño, la interpretación ganará coherencia; para ello, exige inversión en peritajes y protocolos.

De manera crítica, el estudio crítico entre Argentina, Brasil, Chile, Estados Unidos y México el cual se va a evaluar revela patrones repetidos y enseñanzas prácticas que sirven para Colombia. Tal fragmentación normativa manifiesta con tipos desordenados o superpuestos, suele generar inseguridad jurídica y hace necesario establecer "puentes" doctrinales. También se advierte que adherir a acuerdos internacionales como el Convenio de Budapest, sin protocolos técnicos ni salvaguardias procesales definidos, puede agravar los problemas en la obtención y valoración de las pruebas y en la protección de garantías. La articulación entre actores públicos y privados a partir de las bases centralizadas y convenios con bancos se detecta como clave para la eficacia de la investigación. Al aplicarlo al caso colombiano, entre 2022 y 2025, la Ley 1273 de 2009 ha sido un marco útil pero parcial: Tutela conceptualmente bienes importantes y permitió imputaciones, pero su efecto preventivo y su manifestación en sentencias con capacidad disuasoria se ha visto limitados por deficiencias institucionales, la falta de homogeneidad en los protocolos de peritaje y la ausencia de instrumentos regulatorios obligatorios sobre retención y reporte mínimo de incidentes por actores clave. Estas conclusiones que combinan lo doctrinal y lo empírico, sostienen que la verdadera tarea no es solo cambiar el fondo de la ley sino recuperar retos técnicos y de gobernanza interinstitucional.

En definitiva, la fuerza práctica de este capítulo, y por qué es conveniente incorporarlo en este ejercicio académico, consiste en la fuerza crítica basada en datos y en la jurisprudencia que enlaza lo normativo con lo operativo. Se propone ofrecer una lista de recomendaciones concretas y factibles: En primer lugar, existen precisiones normativas concretas para eliminar los vacíos interpretativos del tipo penal sin ampliar la punibilidad; en segunda instancia, están los protocolos nacionales para la preservación y las cadenas de custodia digital validados por laboratorios forenses acreditados; un tercer ítem, serían los mecanismos de cooperación 24 / 7 y clausulas modelos para acuerdos con proveedores extranjeros que salvaguarden la evidencia transfronteriza; un cuarto elemento, sería la obligación del reporte de incidentes y requisitos mínimos de incidentes y estándares mínimos de retención para actores financieros y plataformas crítico; y por último, está la inversión sostenida en plataformas de análisis de fraude y en la capacitación de jueces y fiscales. Sin embargo, no se trata solo de aumentar, sino de reforzar la prevención, la detección temprana y la eficacia procesal; lo cual podría resultar en una reducción del hurto por medios informáticos y en mayor confianza en la respuesta estatal. En conclusión, la Ley 1273 de 2009 se mantiene vigente, pero para el periodo entre 2022 y 2025 requiere protocolos, recursos y armonización normativa que la convierten en una herramienta operativa.

3.1. De la práctica argentina a la política criminal colombiana frente al hurto por medios informáticos

Desde finales del siglo XX, Argentina se puso a ajustar sus normas y la doctrina para enfrentar las nuevas formas de delincuencia vinculadas a las TIC´s. Inicialmente, se dictaron normas sobre confidencialidad y protección del software, se trabajó la propiedad intelectual, y con el tiempo aparecieron tipos penales específicos que cubren otras conductas que en otros lugares se agrupan bajo "hurto informático". Así como, los investigadores que siguen ese avance normativo destacan como el sistema penal argentino fueron sumando marcos sectoriales como la Ley 24.766, la 25.326, la 25.930 y la 26.388; hasta articular una respuesta más amplia con la incorporación al Convenio de Budapest por medio de la Ley 27.411. Así se configuró en una estructura que fusiona las mezclas definiciones técnicas, reglas de privacidad y figuras penales destinadas a proteger sistemas y datos. A pesar de ello, este esqueleto legislativo, si bien amplia el repertorio punitivo, trae consigo problemas de coherencia y coordinación que condicionan la eficacia de la persecución cuando se trata de hurto por medios informáticos (Arocena, 2012; Pilmayquén Reina, 2013: Presidencia de la Nación Argentina – Ley 27.411, 2018).

En el ámbito de tipicidad, Argentina no cuenta con una figura llamada “hurto informático”; en consecuencia, la persecución de conductas que suponen la sustracción patrimonial por medios digitales se realiza a través de la articulación de múltiples tipos: La defraudación por técnicas informáticas (Inciso 16 del Artículo 173); los daños a datos y sistemas (artículos 183 y 184) y las figuras relativas al acceso no autorizado y la violación de comunicaciones (Artículo 153 y siguientes), entre otros. La Ley 26.388 aportó modernizaciones al Código Penal introduciendo conceptos como documento digital, firma y soporte electrónico y desarrollando capítulos sobre la vulneración de secretos y la privacidad, lo que facilita encuadrar conductas que en otros ordenamientos serían consideradas hurto cibernético. Sin embargo, esa dispersión normativa exige que el investigador y el juzgador articulen normas y principios para definir la conducta típica, su elemento subjetivo y las consecuencias penales aplicables, complicando así la previsibilidad y la uniformidad de la respuesta punitiva (Arocena, 2012, pp. 945 - 988; Pilmayquén Reina, 2013, pp. 7 - 11).

Así pues, mediante la Ley 27.411, aprobada en 2018, Argentina se incorporó al Convenio de Budapest, integrando su ordenamiento legal mecanismos de cooperación internacional, procedimientos para alcanzar pruebas en el extranjero y orientaciones técnicas para combatir el cibercrimen. Pese a ello, la medida no estuvo exenta de críticas; desde la sociedad civil y la academia se advirtió que algunas formulaciones eran excesivamente generales, lo que podría generar riesgos para investigaciones legítimas de ciberseguridad o propiciar lecturas arbitrarias. Frente a estas críticas, el Estado formulo reservas, en especial al hurto informático y la jurisdicción penal, y ha sostenido la presencia activa en el *Cybercrime Convention Committee* (CT-Y), en español Comité del Convenio sobre la Ciberdelincuencia, como parte de su estrategia contra los delitos informáticos. Sin embargo, estas reservas y cuestionamientos reflejan la tensión entre garantizar la eficacia investigativa y proteger derechos y prácticas técnicas locales, de modo que la adhesión, por sí sola, no asegura una persecución más eficiente del hurto informático sin protocolos y salvaguardas procesales (Hertler, 2024, p. 15; Infobae, 2018; Martins dos Santos, 2022; Presidencia de la Nación Argentina – Ley 27.411, 2018).

En el plano procedimental y de técnicas de investigación, la literatura jurídica argentina demuestra que los cambios sustantivos en materia legal no siempre han estado acompañados de una modernización proporcional en protocolos y métodos forenses aplicable a la evidencia digital. Varios estudios especializados indican que la investigación de este tipo de ilícitos requiere salvaguardia probatoria estricta, cadena de custodia digital bien documentadas, técnicas específicas de preservación y mecanismos claros de cooperación internacional. Sin regulación específica ni capacitación adecuada, tanto las fuerzas de seguridad como el Ministerio Pública enfrentan dificultades para asegurar pruebas sólidas y presentar imputaciones con alta probabilidad de éxito. Chales plantea que las herramientas de investigación deben a ajustarse a garantías y estándares técnicas, mientras que, Arocena enfatiza que las figuras penales necesitan prácticas estandarizadas para ser operativas en supuestos de defraudación y acceso ilegítimo (Arocena, 2012; Chales, 2018). La carencia de guías procedimentales y la insuficiente capacitación en peritaje digital explican la diversidad de resultados observada en procesos semejantes.

Uno de los temas más polémicos ha generado en Argentina es la amenaza que representan las normas redactadas de forma excesivamente amplia para la investigación en seguridad informática y el ejercicio del *white – hat research*. Las advertencias surgieron con fuerza durante el proceso de adhesión al Convenio de Budapest, cuando organizaciones de la sociedad civil y especialistas señalaron que algunas cláusulas podían disuadir la detección y divulgación responsable de las vulnerabilidades técnicas, abriendo la puerta a interpretaciones penales de actividades legítimas. Estas inquietudes se plasmaron en reservas oficiales y en críticas difundidas en el ámbito mediático y académico, las cuales subrayan la urgencia de prever garantías expresas como, por ejemplo, excepciones legales, protocolos de unificación y criterios claros para valorar la intención. Ignorar este ajuste podría afectar la colaboración entre instituciones académicas, empresas y autoridades,

reduciendo la eficacia de prevención y detección de fallos tecnológicos (Hertler, 2024, pp. 15 – 16; Infobae, 2018; Martins dos Santos, 2022).

En cuanto a las prácticas delictivas y la información empírica disponible, distintos estudios técnicos muestran que las principales modalidades de "hurto informático" en el terreno económico están fuertemente relacionadas con técnicas de Ingeniería Social tales como el *Phishing*, *Smishing* y fraudes basados en el robo de credenciales, además de ataques que aprovechan vulnerabilidades en plataformas de servicios financieros y *fintech*. Adicionalmente, los trabajos académicos y artículos recientes presentadas en eventos académicos destacan un crecimiento continuo de esas prácticas y el surgimiento de nuevos vectores de ataque relacionados con la expansión de la inclusión financiera digital, que expone a más usuarios a este tipo de fraudes. En el campo *fintech,* se destaca que la multiplicación de actores, el uso de procesos de registro completamente digitales y la interconexión de plataformas amplían la superficie del ataque. Entre las medidas propuestas, la doctrina subraya la obligatoriedad de notificar incidentes, el establecimiento de requisitos mínimos de seguridad y la observación activa entre el sector público y privado para reducir la victimización y optimizar la investigación de delitos patrimoniales por medios informáticos (Penna et al., 2022; Negro, 2023; Amato, 2024).

Un repaso crítico de la respuesta argentina al hurto por medios informáticos permite ver logros claros y sombras relevantes. Entre los primeros se cuenta la modernización del ordenamiento penal, incluyendo figuras sobre el acceso ilegítimo, el daño informático y la defraudación digital; la puesta en funcionamiento de canales de cooperación internacional y una mayor sensibilización institucional sobre la ciberseguridad. En contraste, las principales limitaciones esta fragmentación normativa que obliga a enlazar tipos para construir imputaciones coherentes; la escasa concreción de procedimientos técnicos y parciales; el riesgo de inhibir la investigación legítima para el empleo de redacciones amplias; y la falta de medidas regulatorias preventivas incorporadas al diseño penal como son las obligaciones de seguridad para proveedores, protocolos de notificación y campañas preventivas. Estas limitaciones menguan la eficacia del castigo en su función preventiva y confirman la necesidad de complementar la represión con instrumentos técnicos – regulatorios y formación especializada (Arocena, 2012; Chales, 2018; Hertler, 2024; Pilmayquén Reina, 2013).

Por último, las enseñanzas de la experiencia argentina derivan en recomendaciones aplicables en Colombia. Primero, la tipificación penal debe ser enlazada a protocolos procesales y a una capacidad forense concreta con el fin de crear tipos sin peritos ni procedimientos estandarizados no es suficiente. Segundo, incluir salvaguardas normativas explícitas que resguarden la investigación legítima en ciberseguridad y no desincentiven la pericia técnica. En tercer lugar, la cooperación internacional requiere negociarse con reservas y con protocolos técnicos que garanticen la preservación y la validez probatoria transfronteriza. Cuarto, la política criminal ha de integrarse con instrumentos regulatorios como requisitos de seguridad para proveedores financieros y obligaciones de notificación, y con programas orientados a poblaciones vulnerables al *Phishing*. Adoptadas en conjunto, estas cuatro líneas favorecen una respuesta multidimensional en Colombia que combine sanción, prevención y fortalecimiento institucional (Hertler, 2024; Martins dos Santos, 2022; Negro, 2023; Penna et al., 2022).

3.2. El modelo brasileño frente al hurto por medios electrónicos y sus implicaciones para el caso colombiano

Este país suramericano no siguió la vía de crear un único código especial contra la delincuencia informática; más bien, ha sido ajustado puntualmente al Código Penal y varías normas sectoriales, como el Marco Civil de Internet; la Ley No. 13.709 de 2018 o la Ley General de Protección de Datos (LGPD) y reglas bancarias. Gracias a eso, delitos como el hurto por vías digitales se encuadran usando figuras tradicionales adaptadas, como, por ejemplo, son el hurto o robo por vía electrónica (Artículo 155, §§ 4º-B y 4º-C), el fraude electrónico (Artículo 171, §§ 2º-A y 2º-B); y la invasión de dispositivos (Artículo 154 – A). La ventaja es la flexibilidad para abordar conductas variadas sin inventar un

bloque legal aparte; la desventaja es que esa dispersión normativa genera dudas conceptuales y operativas que complican la certidumbre penal y la alineación con estándares externos (Martins Dos Santos, 2022, pp. 19 – 20; Ministerio de la Presidencia de Costa Rica & Instituto Costarricense de Drogas, 2022, pp. 9 – 10).

En el ámbito procesal, la normativa brasileña incorpora múltiples herramientas tecnológicas para la investigación como la conservación de registros de conexión y acceso a aplicaciones; interceptaciones en casos graves a través de la geolocalización y uso de micrófonos con autorización judicial; y, la posibilidad que la Policía Federal actúe como un punto de enlace 24 / 7 en la cooperación internacional, lo cual facilita reunir *e-vidence* en casos de hurtos informáticos. No obstante, existen "cuellos de botella" prácticos tales como la tramitación de rogatorias pueden atrasar el acceso a datos en servidores en el extranjero; y se discute en la *Ação Declaratória de Constitucionalidade* No. 51(ADC 51) del Supremo Tribunal Federal (STF) si es posible requerir información directamente a empresas tecnológicas en el exterior sin recurrir a la cooperación internacional. Tales tensiones repercuten en la eficacia real de la persecución transnacional del delito (Martins Dos Santos, 2022, pp. 31 – 34, STF, Audiencia No. 29, 2020).

Así pues, las obligaciones de preservar y retener datos constituyen una herramienta procesal valiosa: El Marco Civil de Internet impone guarda los registros de conexión por un año y los de acceso a aplicaciones por seis meses, con la alternativa de órdenes judiciales para períodos superiores (Martins Dos Santos, 2022, p. 28). Eso facilita la reconstrucción de hechos en fraudes y hurtos electrónicos, aunque su eficacia práctica está ligada a la cooperación de los proveedores y a una implementación técnica uniforme como es la retención, salvaguardia y cadena de custodia (Martins Dos Santos, 2022, p. 37). Además, la falta de una regulación técnica y una doctrina desarrollada sobre la custodia de criptomonedas y dispositivos incautados deja huecos relevantes en investigaciones donde el hurto informático se articula con el lavado de activo o *ransonwares* (Martins Dos Santos, 2022, pp. 54 - 55).

Desde la perspectiva institucional, Brasil registra avances con claro efecto operativo. La Policía Federal mantiene unidas especializadas en delitos informáticos y programas consolidados como el Proyecto Tentáculos, la cual consiste en una base nacional de fraude bancario electrónico gestionada con la Federación Brasileña de Bancos (FEBRABAN); ya ha firmado convenios con el sector bancario brasilero que posibilitan centralizar datos y detectar patrones de fraude entre estados, evitando la dispersión investigativa. Estas alianzas público – privadas y la creación de la *Base Nacional de Fraudes Bancárias Eletrônicas* (BNFE) han dado resultados eficaces contra redes organizadas que cometen hurtos en todo el país; la coordinación con FEBRABAN y *Caixa Econômica Federal* (CAIXA) mejora la investigación y la prosecución penal más efectiva (Martins dos Santos, 2022, pp. 45–46; cisoadvisor, 2022).

Por otro lado, la adhesión apresurada de Brasil al Convenio de Budapest, sin un proceso de deliberación multisectorial suficientemente amplio, fue objeto de críticas por parte de organizaciones de la sociedad civil de este país. Adicionalmente, entre otros temas de debates se encuentran la insuficiencia de salvaguardias procesales y la falta de alineación regulatoria con estándares de DDHH y de protección de datos aplicables a la investigación penal. Aún cuando en el Congreso aprobó la adhesión mediante el Decreto Legislativo No. 37 de 2021, todavía no se ha completado la ratificación en el plano internacional ni la implementación plena, que exige ajustes tanto legales como administrativos para asegurar su coherencia con el orden interno y con las garantías constitucionales. Este conjunto de críticas evidencia que la efectividad en la lucha contra la criminalidad no puede sacrificar la legitimidad democrática ni el respeto a las garantías procesales, pues, sin estos elementos no es posible asegurar el respaldo social duradero y una sólida seguridad jurídica (Carta Coalizão Direitos na Rede, 2021; Martins dos Santos, 2022, pp. 20–21).

Haciendo referencia a los resultados y estadísticas, el panorama no del todo claro, pues las fuentes consultadas ofrecen datos que siempre coinciden. Por un lado, se documenta un crecimiento en la complejidad del cibercrimen, en casos de *ransonware* y fraudes bancarios organizados que así lo demuestran. Por otro, existen registro que evidencian un descenso en las denuncias en determinados períodos, como, por ejemplo, un informe de febrero de 2025 mostro que en Brasil hubo una reducción del treinta y tres por ciento (33%). Este tipo de situaciones podría explicarse por subregistros, cambios en los hábitos de denuncia o preferencia por canales alternativos como los bancos, que no forman parte de la denuncia penal tradicional. Así, sin un estudio estadístico detallado y coherente, es difícil determinar con precisión la verdadera eficacia de las herramientas legales (InsightCrime, 2024; Cruz, 2025).

Entre tanto, las enseñanzas extraíbles del modelo propuesto por el gobierno brasileño para el sistema punitivo colombiano para el periodo entre 2022 y 2025, se puede afirmar que inicialmente estaría la combinación de reformas que adapten las figuras delictivas existentes con marcos normativos sectoriales como son las de protección de datos o regulaciones civiles lo cual pueda generar un margen de acción flexible, siempre que se acompañe de un trabajo riguroso de definición conceptual que elimine ambigüedades y refuerce la certeza jurídica. En segunda instancia, el establecimiento de acuerdos operativos con el sector financiero y el uso de base de datos centralizadas, como el BNFBE o el Proyecto Tentáculos, incrementa notablemente la efectividad investigativa contra los hurtos informáticos organizados (Martins dos Santos, 2022, pp. 31–37). Un tercer punto a tener en cuenta consiste en la posibilidad de coordinar acciones permanentes y un plan de formación continua para equipos especializados amplifica la eficacia de la respuesta penal. En cuarta instancia, toda adhesión e instrumentos internacionales, como el Convenio de Budapest, debe ser acompañada de un proceso de armonización legal y de garantías procedimentales que preservan derechos fundamentales y confianza social. Por último, es indispensable contar con normas específicas sobre custodia de criptomonedas y preservación técnica de evidencia para prevenir vacíos legales en investigaciones que involucren activos digitales (Japiassú & Costa, 2013; Martins dos Santos, 2022, pp. 45 – 46; Peralis Security).

El modelo brasileño frente al hurto informático refleja un desarrollo normativo e institucional normativo avanzado, que combina adecuaciones en la tipificación penal, herramientas procesales modernas y APP's efectivas. Pese a ello, su alcance pleno se ve coordinado por problemas en la cooperación internacional, limitaciones técnicas en la custodia de criptomonedas; y, controversias políticas y sociales sobre la forma de implementar estándares internacionales (Martins dos Santos, 2022, pp. 28 -37). Aun así, su rendimiento pleno se ve limitado por dificultades en cooperación internacional, carencias técnicas como la parte de regulación sobre criptoactivos y tensiones sociopolíticas por la adopción de pautas internacionales. Para Colombia, se aconseja una fórmula que combine especialización institucional y la cooperación financiera, con una legislación clara de garantía de derechos y protocolos técnicos para la custodia de evidencias, sumando capacitación y mejoras tecnológicas permanentes. (Martins dos Santos, 2022, pp. 45–46; Ministerio de la Presidencia e Instituto Costarricense de Drogas, 2022, pp. 9–10).

3.3. La evolución normativa e institucional de Chile frente al hurto por medios informáticos

A pesar de que el sistema jurídico chileno tiene una larga *data*, sin embargo, su desarrollo en materia de delitos informáticos ha tenido una evolución hasta fechas recientes algo retrasado frente a las exigencias de la era digital. En este contexto, una de las normativas pioneras en tierras australes fue la Ley No. 19.223 de 1993 mediante la cual se tipificaron conductas vinculadas a sistemas de información como la falsificación de datos, el hurto y la divulgación maliciosa de información, y sentó las bases de un tratamiento penal específico del problema (Martins Dos Santos, 2022, p. 15). Pronto, la práctica institucional y la doctrina señalaron que era necesario adaptar en evidencia pronto la necesidad de modernizar las figuras penales y dotar de herramientas procesales adecuadas para casos que ocurren en ambientes digitales complejos. En ese proceso de modernización, la alineación

del Convenio de Budapest y la promulgación de normas más avanzadas, en especial la Ley No. 21.459 de 2022, suponen una modificación importante del panorama legislativo (Martins Dos Santos, 2022, p, 27). Esta actualización incorpora figuras penales, reglas procesales específicas y mecanismos que buscan facilitar las investigaciones tecnológicas. No obstante, solo con el paso del tiempo y con datos empíricos se podrá valorar si estas reformas han impactado de forma real en la reducción del hurto informático (Cavada Herrera, 2020).

La adhesión de Chile al Convenio de Budapest se concretó en 2017 y empezó a aplicarse el 1 de agosto de ese año, lo que implicó un compromiso con la cooperación internacional contra el derecho informático. Sin embargo, la ratificación incluyo reservas considerables que limitan la extensión operativa de algunas obligaciones del Tratado. El texto de la adhesión dejó fuera normas relacionadas con la ley nacional, aspectos jurisdiccionales y delitos como la pornografía infantil, y permitió negar asistencia internacional cuando la conducta no esté recogida con la legislación interna (Martins Dos Santos, 2024, p. 24). Esto en la práctica, disminuye la certidumbre sobre la cooperación internacional para acceder y preservar datos, un problema serio en hurtos informáticos donde la prueba suele encontrarse fuera de la jurisdicción local. En conclusión, la adhesión con reservas evidencia la tensión entre integrarse a sistemas cooperativos y cautelar la autonomía interna, lo que limita la eficacia frente a delitos de corte transnacional (Martins Dos Santos, 2024, p. 57).

En el plano institucional, Chile cuenta con una estructura relativamente sólida para enfrentar los ciberdelitos del Ministerio Público dirige las investigaciones y ejerce la acción penal pública; la Policía de Investigaciones (PDI) tiene brigadas especializadas como la Brigada Metropolitana de Ciberdelitos, la cual funciona desde 2000; y el país dispone de un Centro de Respuesta a Incidentes de Seguridad Informática de Chile (CSIRT- CL) adscrito al Ministerio del Interior y de la Seguridad Pública, que presta asistencia técnica y protege infraestructuras estratégicas (Cavada Herrera, 2020; Martins Dos Santos, 2024, pp. 6 – 7). A lo anterior se suman unidades como la Unidad de Lavado de Dinero, Delitos Económicos, Medioambientales y Cibercrimen (ULDECO) del Ministerio Público que ofrece capacitación a fiscales y asesores especializados; y la Unidad de Cooperación Internacional y Extradiciones (UCIEX), encargada de la cooperación internacional (Martins Dos Santos, 2024, p, 28). No obstante, la sola existencia de esas instituciones no asegura una persecución eficaz del hurto por medios informáticos: Se requiere un plan de formación continuo, peritos forenses suficientes y bien entrenados, protocolos claros para la conservación y cadena de custodia de evidencia digital, recursos técnicos y financieros apropiados. En definitiva, aunque hay veces formales y capacidades técnicas relevantes, mejorar el desempeño operativo exige inversión continua, coordinación entre organismos y sistemas de evaluación basados en estadísticas más detalladas (Martins Dos Santos, 2022, p. 34; Cavada Herrera, 2020).

Las reformas procesales introducidas por la Ley No. 21.459, y discutidas a través del PL – 12.192 – 95 reavivaron temas esenciales sobre conciliar la eficacia investigativa y protección de derechos fundamentales. Por un lado, la normativa ofrece instrumentos para normalizar pesquisas, como reglas para la conservación de datos, facultades vinculadas al decomiso y el comiso por equivalencia y vías para articular la cooperación técnica con proveedores y autoridades extranjeras (Martins Dos Santos, 2022, p. 21). Pero en la tramitación surgieron también propuestas polémicas, que fueron rechazadas, dado que habrían recortado controles, por ejemplo, permitiendo al Ministerio Público pedir datos o flexibilizar el régimen del Artículo 219 relativo a las interceptaciones comunicativas (Martins Dos Santos. 2022, pp. 25 – 26). El rechazo de estas propuestas indica que la sociedad y al legislador demandan que la modernización vaya acompañada de salvaguardas procesales explícitas, límites temporales, supervisión judicial y mayor transparencia en la cooperación de terceros.

En cuanto a cooperación internacional y a la persecución del componente económico del hurto informático, Chile ha establecido canales técnicos y jurídicos concretos: Cuando el Estado requerido no es parte del Convenio de Budapest utiliza una Red 24 / 7 para pedir la preservación de datos, y cuando aplica recurre el punto de contacto de la Convención, adicionalmente, la Unidad de Análisis

Financiero puede recibir reportes sobre operaciones sospechosas relacionadas con los delitos incorporados por la Ley 21.549, lo que permite perseguir la dimensión patrimonial y posibles conductas de lavado (Martins Dos Santos, 2024, p. 37). Dicho esto, la eficacia real depende de la interoperabilidad de los sistemas del reconocimiento recíproco de solicitudes y de que no existan vacíos jurídicos que permitan eludir responsabilidades. El balance práctico es, por ende, mixto dado los instrumentos como la preservación, comiso y reportes; pero su operatividad esta condicionada a la diplomacia, la cooperación de otros Estados y la capacidad técnica chilena para traducir esas medidas en evidencias y sanciones efectivas (Martins Dos Santos, 2022, p. 42).

Para sintetizar, se presentan cuatro lecciones aplicables al caso colombiano a partir del material revisado. Primero, cualquier modernización normativa debe llevar incorporadas salvaguardas procesales como son los controles judiciales, transparencias y límites temporales; que protejan la legitimidad investigativa (Martins Dos Santos, 2022, pp. 25 – 26). Segundo, las herramientas legislativas como tipos, comiso y reglas de preservación; necesitan respaldo en capital humano técnico y protocolos estandarizados de peritaje y cadena de custodia para que la prueba digital sea aceptada y sólida en juicio (Cavada Herrera, 2020). Tercero, la política de adhesión y cooperación internacional tiene que orientarse a reducir reservas que implican la obtención de evidencia transfronteriza; cuando no sea posible eliminarlas, conviene compensar con acuerdos bilaterales o mecanismos 24 / 7 (Martins Dos Santos, 2022, p. 42). Finalmente, la medición de eficacia requiere datos estadísticos desagradados entre 2022 y 2025 sobre denuncias, preservación, procesos y sentencias son esenciales para verificar los resultados (Martins Dos Santos, 2022, p. 15). Estas lecciones permiten al Sistema Penal Colombiano aprendieron de los logros límites chilenos sin replicar soluciones a medias.

3.4. Entre la norma y la práctica. Lecciones de Estados Unidos para evaluar la eficacia de la Ley 1273 de 2009.

El sistema punitivo estadounidense se ha convertido en un punto de referencia clave en el diseño de normas y estructuras contra los delitos informáticos que busca frenar los delitos informáticos, incluido el hurto cometido por medios tecnológicos. Ya que, los estudios revisados destacan que, si bien, no se trató del primer país en legislar sobre estas conductas, marco la diferencia por la prontitud y la profundidad de su regulación; y por consolidar organismos preparados para la prevención, atención y sanción de estas conductas (Narváez Montenegro & Recalde Machado, 2018, p. 6). Así es, como en este apartado se exponen los cambios legislativos penales, donde se muestra las estructuras de entidades dedicadas al tema, explica la caracterización del hurto informático bajo la mirada norteamericana y presenta aprendizajes y límites que resultan valiosos para Colombia en el período entre 2022 y 2025.

Por lo tanto, la evolución normativa en Estados Unidos sobre delitos cibernéticos se inició con el CFAA destinado a combatir amenazas a la información digital, y luego se expandió con reformas. Pues, la reforma de 1994 denominada el *Acta Federal del Abuso Computacional*, la cual reformó la normativa de 1986, siendo determinante, pues, evitó definiciones técnicas sobre "virus", y en cambio, por ejemplo, la transmisión de comandos que dañen sistemas o datos, permitiendo así capturar nuevas formas de ataque sin depender de terminología especializada. Por otra parte, la ley separa responsabilidades, según el grado de culpa, por ejemplo, intencionalidad *versus* temeridad, y contempla penas que, en supuestos graves, pueden llegar hasta diez (10) años de prisión, lo cual favoreció la persecución de autores de virus, o difundían *software* dañino (Candelario Samper & Rodríguez Bolaños, 2015, p. 160; Díaz, 2022, pp. 36 – 38).

De esta manera, el gobierno de los Estados Unidos organizó una red interinstitucional para prevenir, responder y comandar asuntos cibernéticos que se agrupa en la *National Security Agency* (NSA), en español, Agencia Nacional de Seguridad, con sus unidades de cibercomando; el *Department of Homeland Security* (DHS), en español, Departamento de Seguridad Nacional, con su área de seguridad cibernética; y, el *United States Computer Emergency Readiness Team* (US – CERT) y

oficinas especializadas de la Casa Blanca, que funciona como una red de prevención y comando. De la misma manera, la Estrategia Internacional para el Ciberespacio de mayo de 2011 y los documentos presidenciales posteriores consolidaron una política amplia que fusiona las medidas de prevención, mecanismos de disuasión, respuestas ágiles y cooperación internacional. Esa estructura coloca el ciberespacio en el centro del poder nacional y orienta políticas que integran capacidades militares y orienta políticas que integran capacidades militares, de inteligencia, diplomáticas y de justicia penal. Por ello, la respuesta estatal se organiza de manera coordinada entre distintas instituciones para proteger activos estratégicos en el entorno digital (Aguilar Antonio, 2020, pp. 21 -27; Bolívar Londoño & Carvajal Ríos, 2024, p. 19; Roesener, 2015, pp. 73 – 83; Terán Villafuerte, 2022, p. 10).

Las fuentes consultadas indican que el Derecho Estadounidense emplea una noción amplia del "cibercrimen" abarcando por un lado de las conductas punibles en que lo informático es blanco, como el acceso indebido a base de datos; y por otro los casos donde lo cibernético solo sirve como instrumento, como ocurre con la estafa electrónica. En este terreno, el "hurto por medios informáticos" se tipifica mediante figuras como el acceso no autorizado o *Hacking*, la difusión del *Malware* que facilita la apropiación de información o bienes, el fraude informático y el robo de identidad; además, la ley incorpora conductas conexas como terrorismo, pornografía y delitos contra la propiedad intelectual; cuando se cometen por vías digitales. En definitiva, el enfoque abarca tanto el daño de la integridad o ocupación de sistemas de utilización de dichos sistemas para perpetrar apropiaciones patrimoniales como el *hacking* que permite el desvío de fondos, *Phishing*, etc. (Acurio del Pino, 2016, pp. 5 – 6; Amato, 2014; Biblioteca del Congreso Nacional de Chile, 2014).

Los autores coinciden en que, pese a una regulación amplia y capacidades estatales importantes, las amenazas cibernéticas avanzan más rápido que las respuestas. Las cifras son contundentes cuando en 2017 se registraron mil quinientas setenta y nueve (1.579) brechas en el sector financiero estadounidense, con un crecimiento anual estimado de los cuarenta y cuatro puntos seis por ciento (44.6%) reportes técnicos, también remiten a millones de incidentes y a ritmos enormes de intentos de ataque, las cuales son sesenta mil trescientos doce por minuto, según *Deutsche Telekom.* Igualmente, herramientas como *Digital Attack Map* reportaron miles de DDoS cada día. Por ello, la mera existencia de figuras penales e institucionales que no garantiza la contención del hurto informático: La atribución, la jurisdicción internacional, la rapidez de propagación, los agresores internos y la economía ilícita de *exploits* y *malware* complican tanto la prevención como la persecución efectiva (citando GBA & ITRC, 2018; y Deutsche Telekom, 2018, Aguilar Antonio, 2020, pp. 19 – 22; Narváez Montenegro & Recalde Machado, 2018, p. 6).

Por otro lado, en la práctica, el *Enforcement* estadounidense articula juicios federales, sanciones administrativas y cooperación internacional, entre el Convenio de Budapest, y varios acuerdos bilaterales; sin embargo, existen barreras operativas: Las practicas forenses son caras, la recolección de pruebas depende frecuentemente de empresas privadas y hay un sesgo selectivo en el cual las investigaciones se llevan hasta su sentencia. A esto se suma, la controversia en torno al CFAA y la expresión "*exceeding authorized access*", ha generado controversias doctrinales que afectan la predictibilidad y los criterios jurisprudenciales (Biblioteca del Congreso Nacional de Chile, 2014; UNODC, 2021).

La experiencia de Estados Unidos deja aprendizajes útiles para pensar cómo aplicar mejor la Ley 1273 de 2009 en Colombia. En primer lugar, una tipificación amplia, centrada en conductas y no en taxonomías tecnológicas rígidas, facilita incorporar nuevas formas de hurto informático, aunque exige criterios doctrinales y jurisprudenciales claros para evitar sobregeneralizadores. Segundo, el montaje institucional como son los centros de mando, coordinación entre organizaciones y estrategias, desde donde son necesarias y estrategias necesarias; por ello, es necesario, aunque insuficiente si no se acompaña de una inversión sostenida en capacidad forense, APP´s y mecanismos de reporte y mitigación. En tercer lugar, la eficacia real depende de una cooperación internacional fuerte y de marcos procesales que permitan gestionar evidencia electrónica entre jurisdicciones. Cuarto, disponer

de datos estadísticos y mecanismos de reporte público sobre brechas, denuncias y condenas es indispensable para evaluar la efectividad real entre 2022 y 2025. Sobre la base de estas lecciones se pueden fundamentar recomendaciones dirigidas a fortalecer la prevención y persecución del hurto por medios informáticos (Aguilar Antonio, 2020, pp. 21 – 27; Bolívar Londoño & Carvajal Ríos, 2024, p, 19; Díaz, 2022, pp. 36 – 38).

En resumen, el modelo estadounidense completo, tanto en el ámbito normativo como en lo institucional, que puede servir de referencia para Colombia, pero la práctica demuestra que no alcanza con contar con el CFAA y agencias especializadas para disminuir la incidencia del hurto cibernético. Lo que importa es una ley que se adapte rápido, capacidad forense adecuada, una gobernanza intersectorial eficaz, colaboración internacional, y sobre todo, indicadores públicos fiables para medir prevención, denuncias, investigaciones y condenas. Dichos criterios deben servir para evaluar la efectividad de la Ley 1273 de 2009 y la generación de pautas alternativas.

3.5. Como conciliar la eficacia penal y las garantías democráticas a partir del caso mexicano

El sistema penal mexicano es un paradigma para el caso latinoamericano para analizar como el Estado regula y responde a los delitos informático, incluido el hurto por medios informáticos; su principal característica es una amplia gama de tipos penales y un ordenamiento fragmentado que combina el Código Penal Federal con normas aisladas y estrategias administrativas. Esa arquitectura legal no nació de forma lineal; vino por etapas desde finales del Siglo XX, destacándose la incorporación de tipos penales relacionados con conductas informáticas en 1999, lo que inicio la construcción de un cuerpo normativo que se complementó después con la Ley de Seguridad Nacional de Ciberseguridad, iniciativas administrativas como la Unidad de Gobierno Electrónico (UGEPT), y, documentos estratégicos tale como la Estrategia Nacional de Ciberseguridad (ENCS) de 2017. Esa combinación de normas penales, administrativas y estratégicas explica por qué México tiene varias herramientas formales para perseguir conductas ilícitas en el ciberespacio, y por otro, de una pluralidad que dificulta la coherencia y la previsibilidad jurídica para operadores y ciudadanos (Martins Dos Santos, 2022, pp. 31 – 32; Narváez Montenegro & Recalde Machado, 2017, p. 8), En los hechos, la dispersión de normas implica que el tratamiento del hurto informático puede cambiar según el nivel gubernamental y según la entidad investigadora, lo que presenta desafíos relevantes para unificar criterios, mejorar la coordinación y homogeneizar la capacitación forense a nivel nacional.

Un rasgo esencial del sistema mexicano es la gran amplitud de su catálogo de ciberdelitos, donde se incluye el hurto por medios informáticos inventarios doctrinales y estudios críticos han contabilizado más de doscientos delitos informáticos observables en práctica y la literatura, entre los que se cuentan el acceso no autorizado, *cracking*, *hacking*, revelación de secretos, *phishing*, *spam* y otras formas de manipulación y activos digitales. Esa amplitud ofrece una ventaja clara: Permite que el Derecho Penal abarque conductas nuevas derivadas de la tecnología y se adapta con relativa rapidez. Esa amplitud tiene una ventaja práctica evidente: Posibilita que el Derecho Penal abarque rápidamente conductas cibernéticas novedosas. Sin embargo, esta multiplicidad también acarrea riesgos cuando las definiciones so vagas o demasiado generales, dado que esa indefinición puede facilitar decisiones judiciales expansivas y producir inseguridad jurídica para usuarios, profesionales y autoridades investigadoras. Por tanto, la amplitud en la tipificación no garantiza por si sola eficacia preventiva ni persecutoria del hurto por medios informáticos; lo que resulta necesario son criterios interpretativos exigentes, técnicas de tipificación bien calibradas y un marco procedimental que delimite con claridad la conducta típica y los estándares probatorios exigibles (Código Penal Federal, 1999; Narváez Montenegro & Recalde Machado, 2018).

La relación entre el Sistema Penal Mexicano y el Convenio de Budapest evidencia las tensiones entre la cooperación internacional y la autonomía normativa: Pese que, en 2006, México solicitó su adhesión, permitiendo así que las ideas y los textos del mismo convenio se limitó al del observador, permitiendo así que las ideas y los textos del Convenio alimenten el debate nacional sin que exista

una transposición sistemática y vinculante. Esa condición crea una doble dinámica: Por un lado, enriquece las reformas con insumos internacionales; por el otro, permite permutaciones parciales que, según especialistas y organizaciones civiles, pueden terminar legitimando respuestas excesivamente punitivas o ampliando facultades de investigación estatal sin las debidas salvaguardas. Por lo tanto, la experiencia mexicana pone de manifiesto invocar estándares internacionales no reemplaza una incorporación reflexivo crítico y democrático que detecte los posibles conflictos con las garantías constitucionales y procesales de orden interno (Martins Dos Santos, 2022, pp. 31 – 35).

Mientras se discutía la adhesión al Convenio de Budapest, México impulso en 2017, la ENCS con objetivos claros: Mejorar la colaboración entre sectores, mapeo de riesgos, promoción de buenas prácticas y refuerzo de capacidades para responder a incidentes de seguridad en el ciberespacio. Esta estrategia constituye un avance en términos de una mirada sistemática, pero la traducción de sus lineamientos a medidas normativas y operativas ha sido controvertida: Se han propuesto por lo menos trece (13) iniciativas legislativas dirigidas a crear una nueva ley marco, a tipificar nuevos delitos y a establecer agencias naciones con funciones preventivas y reactivas. Así es como, organizaciones civiles y grupos académicos han denunciado que muchas de estas iniciativas no integran adecuadamente una perspectiva de DDHH ni contemplan controles y transparencia, advirtiendo que el diseño institucional podría ampliar la vigilancia estatal sin los contrapesos procesales necesarios. En consecuencia, aunque existe una estrategia solida en lo formal, su transformación en normas procesales, protocolos de investigación y una arquitectura institucional operativa todavía tiene vacíos y riesgos que pueden minar la confianza pública y la protección de las libertades (Martins Dos Santos, 2022, p. 32).

Las observaciones provenientes tanto de la sociedad civil como de especialistas en DDHH se han convertido en un punto medular para analizar la solidez democrática de las medidas mexicanas frente a los ciberdelitos. Desde el trabajo de colectivos como la Red en Defensa de los Derechos Digitales (R3D) hasta aportes de diferentes centros de investigación, se ha advertido la existencia de tipos penales redactados con excesiva generalidad, lo cual se traduce en una posible ampliación arbitraria de las competencias de investigación por parte del Estado. Tal situación acarrea riesgos evidentes, particularmente sobre la libertad de expresión y sobre la protección de aquellos que cumplen un papel de alertadores o denunciantes de corrupción. Dicho escenario plantea riesgos inmediatos, entre ellos la vulneración de la libertad de expresión y la ausencia de garantías para quienes denuncian prácticas ilícitas en el espacio digital. Lejos de ser reproches teóricos, tales advertencias apuntan a exigencias concretas sobre cómo debe diseñarse una política criminal como enfoque tecnológico. Por otro lado, los críticos advierten que la adopción de un paradigma centrado casi exclusivamente en la seguridad nacional puede erosionar derechos constitucionales y producir un efecto adverso sobre la confianza ciudadana en las instituciones, alimentando una percepción de desproporcionalidad en el uso del poder punitivo (Carriedo Téllez, 2022; Martins dos Santos, 2022).

Desde un punto de vista operativo, la fractura normativa y la diferencia jurisdiccional federal y lo estatal inciden de manera notable en la persecución del hurto informático: Las capacidades forenses muestran diferencias notables según la región, los protocolos de cooperación interinstitucional adolecen de vacíos y la ausencia de estándares compartidos complica preservan la cadena de custodia y presentar pruebas digitales que sean admisibles de manera uniforme. Consecuentemente, se observan tasas de resolución dispares, itinerarios procesales contradictorios para las víctimas y las limitaciones para desmantelar redes transnacionales que operan con infraestructuras distribuidas. Por ende, resulta evidente que la existencia de tipos penales no logra por sí sola mitigar el fenómeno sin una apuesta concomitante por la inversión en capacidades forenses, la capacitación de fiscales y jueces, la armonización de protocolos y la efectividad de la cooperación internacional, los cuales constituyen las brechas más señaladas por las evaluaciones mexicanas (Gobierno de México, 2021; Martins dos Santos, 2022, pp. 31 – 35).

A partir del caso mexicano se desprenden varias lecciones útiles para el contexto colombiano y la lectura crítica de la Ley 1273 de 2009: Primero, evitar la promulgación de tipo penales excesivamente amplios o vagos que provoquen inseguridad jurídica y permiten interpretaciones expansivas. En segundo lugar, la creación o ampliación de tipos penales debe contemplar un plan tangible del fortalecimiento institucional; incluyendo inversión en capacidades forenses, formación de fiscales y jueces y protocolos operativos, para que la respuesta penal sea efectiva. Tercero, desde el diseño de la reforma debe incorporarse un enfoque de DDHH que proteja la libertad de expresión, los derechos de los alertadores y el debido proceso. Cuarto, promover la armonización normativa entre niveles de gobierno y articular mecanismos robustos de cooperación internacional es esencial para abordar la dimensión transfronteriza sin sacrificar garantías. En síntesis, la efectividad normativa está coordinada tanto por la calidad técnica de las leyes como la solvencia institucional para aplicarlas respetando las libertades fundamentales (Narváez Montenegro & Recalde Machado, 2018, p. 7; Martins dos Santos, 2022, pp. 31 – 35).

Conclusiones

Esta monografía parte de una pregunta práctica y epistemológica, no retórica ¿Hasta qué punto la Ley 1273 de 2009 ha mostrado entre 2022 y 2025, capacidad real para prevenir, perseguir y sancionar el hurto informático en Colombia? Formularlo así obliga a desplazar la atención desde la norma escrita hacia la experiencia real. Es necesario confrontar la norma con la actuación institucional y con los registros estadísticos de denuncias. La jurisprudencia relevante es otro insumo imprescindible para medir su alcance y sus límites. En términos concretos interesa saber cómo funcionan las unidades forenses y las fiscalías especializadas. También la capacidad de los laboratorios periciales y la articulación con proveedores de servicios digitales. Y, cuando le corresponde, la coordinación con autoridades extranjeras en procesos de remisión y colaboración. No es solamente cuestión de adecuación tipológica entre tipo y conducta en el papel. Hay que ver si la normativa produce prácticas que solucionen casos complejos en tiempos razonables. Por eso la evaluación debe combinar indicadores cuantitativos con criterios cualitativos sobre calidad y procedimiento. En resumen, la pregunta guía tanto la recolección de evidencia como el estándar de evaluación aplicado.

Ahora bien, haciendo referencia sobre el objetivo general de este ejercicio reflexivo es analizar de manera crítica la eficacia de las herramientas jurídico – procesales contenidas en la Ley 1273 de 2009 durante el período entre 2022 y 2025. Sin embargo, pese de pretender ser un objetivo "políticamente correcto", este propósito actúa como criterio de priorización. Por ello, se determina, por ejemplo, cuales fuentes y pruebas pesan en la argumentación. Por ello, es necesario analizar sentencias relevantes para calibrar la interpretación judicial. Y determina que estadísticas resulta importante pertinentes para medir la capacidad persecutoria. Sin embargo, en la *praxis* se traduce en elegir fallos que aporten criterios de aplicación y no sólo resoluciones puntuales. En lo que interesa, en particular, la jurisprudencia sobre la admisibilidad de las pruebas digitales. Igualmente, es importante como a partir de la jurisprudencia permite rastrear activos y cuantificar el daño. Por esto mismo, el objetivo obliga a comparar con modelos extranjeros, no para copiar, sino para aprender lecciones. Ya que, si se adaptan esas reformas con criterio, con el propósito de acercar la "letra de la norma" a resultados reales. En definitiva, el objetivo guía tanto la recolección de evidencia como el estándar de la evaluación.

Al mirar las cifras de las denuncias y su tendencia salta a la vista un patrón preocupante: Los altibajos en las denuncias no se traducen automáticamente en más procesos o condenas, lo que revela una desconexión entre quienes buscan justicia y la capacidad del Estado para responder. Esta separación tiene múltiples causas concatenadas como ausencia de peritajes oportunos, la diversidad de protocolos locales para preservar las pruebas, retrasos en las solicitudes internacionales y una dispersión de responsabilidades entre actores públicos y privados. Cada uno de esos elementos contribuye a que el elemento contribuye a que el volumen de denuncias sea, en realidad, un indicador equívoco: Puede significar mayor reincidencia, mayor confianza para denunciar o un sistema que recoge quejas sin darles tramites. Por eso, las cifras una lectura contextual; y esta investigación prioriza indicadores derivados; por ejemplo, la tasa de denuncia; imputación y el tiempo medio de conservación de datos; que son más ilustrativos de la capacidad operativa que la cifra absoluta de denuncias.

El panorama institucional con claridad que la gobernanza frente al hurto informático no se ha consolidado, sino que, opera desde una lógica fragmentaria. La Policía, la Fiscalía y la Superintendencia Financiera aplican criterios distintos que reflejan sus propios marcos internos, sin lograr una verdadera integración. Mientras que los actores privados por medio de plataformas tecnológicas, bancos y proveedores de pago; se rigen por sus propios protocolos de seguridad y gestión de información, sin que ello necesaria contribuya al interés público. La consecuencia inmediata de esta desarticulación es la generación de "puntos ciegos" en la investigación penal. Entre ellos, se destacan cuentas que se eliminan antes que puedan ser asegurados, registros digitales que caducan sin respaldo suficiente y comunicaciones internacionales que entorpecen por no existir

clausulas uniformes que faciliten el intercambio. Esos vacíos que la prueba digital se torne volátil y frágil, afectando la eficacia del sistema de justicia. Ante ello, se sostiene que solo mediante la construcción de una arquitectura de gobernanza sólida, con reglas claras de competencia, canales técnicos uniformes y obligaciones de preservación de datos mínimos, podrá el sistema penal superar la vulnerabilidad de su propia evidencia.

En términos criminológicos, la complejidad del hurto por medios informáticos radica en que no se trata de un tipo de delito homogéneo, sino de una contestación de modalidades que oscilan entre lo rudimentario y lo altamente sofisticado. En el nivel básico encontramos técnicas como el *phishing* o el *vishing*, que requiere poco conocimiento especializado, pero logran gran impacto entre usuarios desprevenidos. En un grado más sofisticado se evidencian ataques organizados que combinan el intercambio ilícito de tarjetas SIM, el blanqueo de capital a través de criptomonedas y la dispersión de operaciones en servicios ubicados en territorios que no facilitan la cooperación internacional.

Cuando se analiza el problema del hurto informático en Colombia, se observa que el factor clave no es únicamente la existencia de normas, sino la manera como estas se acompañan de recursos materiales y programas de formación especializada. Para que la política criminal sea efectiva se requiere complementar la norma con recursos materiales y con formación constante de los actores judiciales. Es necesario que los laboratorios forenses estén bien equipados, que las fiscalías dispongan de personal entrenado y que magistrados y peritos reciban capacitaciones de manera constante. Cuando se analizan los casos de otros países, queda claro que aquellos que han destinado recursos a consolidar redes de laboratorio y a fomentar la colaboración con el sector privado han logrado mejores resultados en el ámbito procesal. En consecuencia, el planteamiento que se desarrolla en este ejercicio reflexivo es que la política criminal debería contemplar una agenda de inversión estable, con objetivos verificables y revisiones periódicas. Además, la capacitación no puede ser vista como un evento esporádico, sino que, debe consolidarse como parte de un sistema nacional de acreditación, lo que contribuiría a fortalecer la credibilidad y eficacia de la justicia digital.

Para esto, resulta necesario la aparición de la cooperación internacional en este escenario, ya que, no se puede solamente remitir al Convenio de Budapest de manera teórica, sino que, se materializa por medio de compromisos y acciones concretas. Por ello, se requiere dar un paso más allá y convertir tales compromisos en herramientas aplicables, como son la conformación de equipos de investigación conformados por distintos países, mediante unos acuerdos de asistencia disponibles las 24 horas del día y los siete días de la semana y disposiciones contractuales con proveedores foráneos que permitan acceder a datos de manera ágil, considerando lo efímero de la información digital. Dado que, cuando las gestiones administrativas son lentas o países carecen de formatos de solicitud claros, los rastros digitales, que son por naturaleza efímeros se pierden con facilidad, provocando que investigaciones potencialmente exitosas concluyan en archivos técnicos.

En la aplicación normativa penal informática se observa un fenómeno de especial preocupación, la cual consiste en el uso recurrente de la reclasificación de las conductas informáticas en delitos clásicos, como el hurto o la estafa, lo cual parece aparece entonces como recurso para sortear la carencia de pruebas técnicas o la falta de peritajes forenses adecuados. Y, en consecuencia, se convierte en un camino procesal más seguro. No obstante, si bien esta solución procesal puede ofrecer un alivio inmediato, a mediano plazo genera consecuencias indeseables: Empobrece la especialidad del Derecho Penal Informático, pues, la Ley 1273 de 2009 pierde vigencia práctica y se limita a la creación de la doctrina jurisprudencial en la materia. Por ello, en vez de reforzar la especificidad normativa, se produce una tendencia regresiva que diluye la autonomía conceptual de los delitos informáticos. Por ello, se insiste en el recurso a figuras tradicionales debe ser subsidiario y justificado con detalle, nunca un camino cómodo o preferente, de modo que no desdibuje la tipicidad propia de los ciberdelitos ni se obstaculice el desarrollo de un Derecho Penal Especializado en tecnologías.

No se intenta aquí formular una conclusión general, sino una respuesta práctica: La Ley 1273 de 2009 mantiene su base conceptual, pero su efectividad entre 2022 y 2025 ha quedado limitada por problemas institucionales, debilidades probatorias y un déficit de gobernanza. El verdadero reto no consiste en reinventar la norma, sino en levantar una base técnico – jurídica que garantice su funcionamiento, lo que implica laboratorios forenses acreditados, protocolos de actuación claros, sistemas de acreditación y un marco de cooperación internacional confiable. Si esos factores se atienden con metas precisas y respaldo financiero, será posible reducir la distancia entre la tipificación y los resultados en caso contrario, la Ley continuará siendo una promesa normativa que no consigue traducirse en capacidad efectiva del Estado para combatir el hurto informático.

Bibliografía

Acosta, M. G., Benavides, M. M., & García, N. P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia, 25*(89). https://www.redalyc.org/journal/290/29062641023/29062641023.pdf

Acurio Del Pino, S. (2016). *Delitos informáticos: Generalidades*. Pontificia Universidad Católica del Ecuador. https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Aguiar, T. (s. f.). *Políticas de ciberseguridad en Brasil: ¿De dónde venimos y hacia dónde vamos?* LACNIC. https://www.lacnic.net/innovaportal/file/6972/1/politicas-de-seguranca-cibernetica-no-brasil-de-onde-viemos-e-para-onde-vamos-thais-helena-aguiar-es.pdf

Aguilar Antonio, J. M. (2020). La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. *Revista de Estudios en Seguridad Internacional, 6*(2), 17–43. https://seguridadinternacional.es/resi/html/la-brecha-de-ciberseguridad-en-america-latina-frente-al-contexto-global-de-ciberamenazas/

Aguilar Antonio, J. M. (2020). La brecha de ciberseguridad en América Latina frente al contexto global de ciberamenazas. *Revista de Estudios en Seguridad Internacional, 6*(2), 17–43. https://seguridadinternacional.es/resi/html/la-brecha-de-ciberseguridad-en-america-latina-frente-al-contexto-global-de-ciberamenazas/

Alcalá Casillas, M. G. (2023). Desafíos en México sobre la regulación de los ciberdelitos. *Derecom, 35*, 1–15. https://dialnet.unirioja.es/descarga/articulo/9352234.pdf

Alcalá Casillas, M. G., & Meléndez Ehrenzweig, M. Á. (2023). Delitos informáticos en México: Reconocimiento en los ordenamientos penales de las entidades mexicanas. *PAAKA, 13*(2). https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-36072023000100005

Amato, M. I. (2024). Cibercrimen y delitos informáticos. *Revista Iberoamericana de Derecho, Cultura y Ambiente, 5*. https://aidca.org/wp-content/uploads/2024/07/RIDCA5-PENAL-AMATO-CIBERCRIMEN-Y-DELITOS-INFORMATICOS.pdf

Amaya-Cristancho, H. A., & Cortes Vargas, Y. L. (2011). Administración de la información: Un reto de la investigación criminal del siglo XXI. *Revista Criminalidad, 53*(2), 175–197. https://revistacriminalidad.policia.gov.co:8000/index.php/revcriminalidad/article/view/271/417

Arévalo Fonseca, S. (2022). Prevención en delitos informáticos. *Plataforma Abierta de Libros y Memorias Académicas (PALMA)*, 1–30. https://cipres.sanmateo.edu.co/ojs/index.php/libros/article/view/545/489

Arias, J. (2021). *Delitos informáticos y derecho penal*. Editorial Universitaria.

Arias-Flórez, M. E., Daza-Martínez, L. A., Ojeda-Pérez, J. E., & Rincón-Rodríguez, F. (2011). Delitos informáticos y entorno jurídico vigente en Colombia. *Cuadernos de Contabilidad, 11*(28). https://revistas.javeriana.edu.co/index.php/cuacont/article/view/3176/2416

Armijo Catalán, J., Bouillet Carroza, E., & Delaere, C. (2025). *Reporte ciberseguridad 2025*. eDigital. https://enteldigital.cl/hubfs/ebooks/ciberseguridad/2025/Entel_Digital_Reporte_Ciberseguridad_2025_.pdf

Arnoudo, D. (s. f.). *O Brasil e o Marco Civil da Internet*. Instituto Igarapé. https://igarape.org.br/marcocivil/pt/

Arocena, G. A. (2012). La regulación de los delitos informáticos en el Código Penal argentino: Introducción a la Ley Nacional núm. 26.388. *Boletín Mexicano de Derecho Comparado, 135*, 945–988. https://www.scielo.org.mx/pdf/bmdc/v45n135/v45n135a2.pdf

Asobancaria. (2023). Un enfoque de auditoría para los riesgos cibernéticos. *Banca & Economía, Edición 1426*. https://www.asobancaria.com/wp-content/uploads/2024/05/1426-BE.pdf

Ávila Jiménez, C. C. (2023, Septiembre 14). Las claves de ciberataque masivo en Colombia: solución tardará más de lo esperado. Por el ciberataque hay paralizados más de 2 millones de procesos judiciales. *El Tiempo. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataque-masivo-en-colombia-rama-judicial-y-servicios-de-salud-caidos-que-paso-805846*

Ballestero, F. (2025). La transformación digital y el coste de los ciberataques: De mejorar la protección a reforzar la ciberresiliencia. *ICE, Revista de Economía, (938)*. https://www.revistasice.com/index.php/ICE/article/view/7891/7989

Banco Interamericano de Desarrollo & Organización de los Estados Americanos. (2020). *Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe*. https://publications.iadb.org/es/publications/spanish/viewer/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf

Barbosa Delgado, F., & Mancera, M. J. (2024). *Informe de gestión 2020–2024: En la calle y en los territorios*. Fiscalía General de la Nación. https://www.fiscalia.gov.co/colombia/wp-content/uploads/Informe-de-gestion-2020-2024-consolidado.-final_18_12_23.pdf

Barrios Solano, S. (2012). *El delito informático en la legislación colombiana*. Corporación Universitaria de la Costa. https://repositorio.cuc.edu.co/server/api/core/bitstreams/f207e22e-7291-4738-82fb-0c33a5a10079/content

Bascur, G., & Peña, R. (2022). Los delitos informáticos en Chile: tipos delictivos, sanciones y reglas procesales de la Ley 21.459 — primera parte. *Revista de Estudios de Justicia, (37)*, 1–37. https://rej.uchile.cl/index.php/RECEJ/article/view/67885/75898

Becerra, J., Cotino Hueso, L., García Vargas, C. B., Sánchez Acevedo, M. E., & Torres Ávila, J. (2015). *La responsabilidad del Estado por la utilización de las tecnologías de la información y la comunicación (TIC)*. Universidad Católica de Colombia. https://repository.ucatolica.edu.co/entities/publication/07e55e96-df58-44fe-af94-187901f65590

Benvenuto Vera, Á. (2004). Los delitos informáticos (Ley 19.223 — Chile) y la función de auditoría informática. Ponencia en la Conferencia Académica Permanente de Investigación Contable. http://www.capic.cl

Biblioteca del Congreso de la Nación (Argentina). (2018). *Legislación y Doctrina Extranjera: Delitos Informáticos (Dossier 063)*. https://bcn.gob.ar/uploads/Dossier-063-Delitos-Informaticos-Actualizacion2018.pdf

Biblioteca del Congreso Nacional de Chile. (2014). *Los delitos cibernéticos en la legislación estadounidense*. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/20864/5/FINAL%20_%20Informe%20_%20Cibercrimen%20en%20EEUU_v5.pdf

Bolaños Díaz, A., & Narváez Narváez, T. de J. (2014). *Análisis comparativo sobre delitos informáticos en Colombia con relación a seis países de Latinoamérica*. Universidad Nacional Abierta y a Distancia (UNAD). https://repository.unad.edu.co/bitstream/handle/10596/2656/59830899.pdf?sequence=1&isAllowed=y

Bolívar Londoño, M., & Carvajal Ríos, V. (2024). *Ciberdelincuencia en Colombia: retos y desafíos jurídicos en la normatividad colombiana*. Universidad Católica Luis Amigó. https://repository.ucatolicaluisamigo.edu.co/server/api/core/bitstreams/f39a9676-ed3a-4955-acd4-f904154aee4e/content

Brasscom. (s. f.). Empresas de tecnologia defendem a adesão do Brasil à Convenção de Budapeste. https://brasscom.org.br/empresas-de-tecnologia-defendem-adesao-do-brasil-a-convencao-de-budapeste/

Brito Cruz, F. de C. (s. f.). *Direito, democracia e cultura digital: a experiência de elaboração legislativa do Marco Civil da Internet* (Tesis de maestría). Faculdade de Direito, Universidade de São Paulo. http://www.internetlab.org.br/wp-content/uploads/2019/04/dissertacao_Francisco_Carvalho_de_Brito_Cruz.pdf

Câmara dos Deputados. (2021). *Relatório do Grupo de Trabalho sobre o PL 2630/2020 (relatório adotado)*. https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/aperfeicoamento-da-legislacao-brasileira-internet/documentos/outros-documentos/relatorio-adotado-do-grupo-de-trabalho

Câmara dos Deputados. (s. f.). *Projeto de lei n. 2126/2011 (Marco Civil da Internet)*. https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=517255

Câmara dos Deputados. (s. f.). *Projeto de lei n. 2630/2020 (Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet)*. https://www.camara.leg.br/propostas-legislativas/2256735

Câmara dos Deputados. (s. f.). *Projeto de lei n. 8045/2010 (Código de Processo Penal)*. https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=490263

Candelario Samper, J. J., & Rodríguez Bolaños, M. (2015). Seguridad informática en el siglo XXI: Una perspectiva jurídico-tecnológica enfocada hacia las organizaciones nacionales y mundiales. *Revista Especializada en Ingeniería, 9*, 133–162. https://hemeroteca.unad.edu.co/index.php/publicaciones-e-investigacion/article/download/1441/1760

Cano Cuervo, A., Díaz Heredia, J. M., Mendieta Vargas, C. C., Rivas Sánchez, C. C., & Sánchez Carvajal, N. F. (s. f.). *Aporte internacional frente a los delitos informáticos en Colombia y su ejecución por parte de las autoridades competentes*. Universidad Libre de Colombia. https://www.pensamientopenal.com.ar/system/files/2015/06/miscelaneas41279.pdf

Carriedo Téllez, L. M. (2022). Delitos informáticos frente a estándares de derechos humanos y libertad de expresión en México. INFOTEC. https://infotec.repositorioinstitucional.mx/jspui/bitstream/1027/518/1/SOLUCIONESTRATEGICA_LMCT.pdf

Carrizosa Acosta, X. L. (2024). *Los retos de la investigación y sanción penal del delito de estafa en espacios digitales* (Trabajo de grado). Universidad Cooperativa de Colombia. https://repository.ucc.edu.co/server/api/core/bitstreams/8ae62387-87af-45c8-8ee2-f3cf77abc2cb/content

Cassou Ruiz, J. E. (2010). Los "delitos informáticos": Situación en México. *Revista del Instituto de la Judicatura Federal, (28)*, 207–236. https://escuelajudicial.cjf.gob.mx/publicaciones/revista/28/Delitos_inform%C3%A1ticos.pdf

Castiblanco Hernández, S. A., Pregonero León, Y. K., Quijano Díaz, A., Rincón Arteaga, J. A., & Urquijo Vanegas, J. D. (2022). Ciberdelincuencia en Colombia: ¿Qué tan eficiente ha sido la Ley de Delitos Informáticos? *Revista Criminalidad, 64*(3), 95–116. http://www.scielo.org.co/pdf/crim/v64n3/1794-3108-crim-64-03-95.pdf

Cavada Herrera, J. P. (2020). Cibercrimen y delito informático: Definiciones en legislación internacional, nacional y extranjera. Biblioteca del Congreso Nacional de Chile. https://obtienearchivo.bcn.cl/obtienearchivo?id=repositorio/10221/29012/2/Definicion_y_regulacion_de_cibercrimen_y_delito_informatico_JPC_edit.pdf

CCIT; Tictac; Safe. (2023). *IA para la protección y prevención de amenazas: Informe anual de ciberseguridad*. https://www.ccit.org.co/wp-content/uploads/estudio-anual-de-ciberseguridad.pdf

Chales, J. P. (2018). *Las técnicas de investigación penal a la luz del Convenio sobre ciberdelito y su aplicación en Argentina* (Tesis de maestría). Universidad Nacional de Cuyo. https://bdigital.uncu.edu.ar/objetos_digitales/19427/1.-chales-juan-pablo-tesis-maestria.pdf

Cifuentes Muñoz, E. (1997). El Hábeas Data en Colombia. *Derecho PUCP*, (51), 115–144. https://doi.org/10.18800/derechopucp.199701.005

Cisoadvisor. (2022, March 24). Governo anuncia plano tático contra cibercrimes. https://www.cisoadvisor.com.br/governo-anuncia-plano-tatico-contra-cibercrimes/

Coalizão Direitos na Rede. (2021, October 21). Carta aos membros do Senado Federal sobre a Convenção de Budapeste. https://direitosnarede.org.br/2021/10/21/carta-aos-membros-do-senado-federal-sobre-a-convencao-de-budapeste/

Comissão de juristas, Câmara dos Deputados. (s. f.). *Anteprojeto da Comissão de Juristas sobre tratamento de dados pessoais na área de segurança pública*. https://www2.camara.leg.br/atividade-legislativa/comissoes/grupos-de-trabalho/56a-legislatura/comissao-de-juristasdados-pessoais-seguranca-publica/documentos/outros-documentos/DADOSAnteprojetocomissaoprotecaodadossegurancapersecucaoFINAL.pdf

Congreso de la Ciudad de México; Instituto de Investigaciones Legislativas del Congreso de la Ciudad de México. (2021). *Ciberseguridad*. https://www.congresocdmx.gob.mx/archivos/legislativas/Ciberseguridad.pdf

Contrera Clunes, A. (2003). Delitos informáticos: Un importante precedente. *Ius et Praxis*. http://www.scielo.cl

Contreras-Manrique, R. de B., Ovalle Lizcano, T. V., Contreras Manrique, L., Coronel Peñuela, D. L., & Rincón Suárez, Z. A. (2023). Tic y los delitos informáticos. *Revista Colombiana de Tecnologías de Avanzada (RCTA), 1*(41), 104–110. https://ojs.unipamplona.edu.co/index.php/rcta/article/view/2511/4599

Colombia. Corte Constitucional. (2019). *Sentencia C-224/19* (Expediente LAT-455; M. P. Cristina Pardo Schlesinger). (https://www.suin-juriscol.gov.co/viewDocument.asp?id=30036578)

Colombia. Corte Constitucional. (2022). *Sentencia T-092/22* (M. P. Paola Andrea Meneses Mosquera). https://www.corteconstitucional.gov.co/relatoria/2022/t-092-22.htm

Colombia. Corte Constitucional. (2022). *Sentencia T-360/22* (M. P. Hernán Correa Cardozo). https://www.revistamisionjuridica.com/la-responsabilidad-objetiva-de-los-bancos-en-los-casos-de-fraude-electronico-en-colombia/

Colombia. Corte Constitucional. (2024). *Sentencia C-030/24*. http://www.secretariasenado.gov.co/senado/basedoc/c-030_2024.html

Colombia. Corte Suprema de Justicia (CSJ). (2016). *Sentencia SC16496-2016* (Radicación n.º 76001 31 03 002 1996 13623 01; M. P. Margarita Cabello Blanco). https://cortesuprema.gov.co/corte/wp-content/uploads/2016/12/SC16496.pdf

Colombia. Corte Suprema de Justicia (CSJ). (2016). *Sentencia SC18614-2016* (Radicación n.º 05001-31-03-001-2008-00312-01; M. P. Ariel Salazar Ramírez). (https://cortesuprema.gov.co/corte/wp-content/uploads/2016/12/SC16496.pdf)

Colombia. Corte Suprema de Justicia (CSJ). (2020). *Sentencia SC5176-2020* (M. P. Luis Alonso Rico Puerta). https://www.revistamisionjuridica.com/la-responsabilidad-objetiva-de-los-bancos-en-los-casos-de-fraude-electronico-en-colombia/

Colombia. Corte Suprema de Justicia. (2021). *Sentencia SP5367-2021* (Radicación n.º 60484). https://edileyer.com/Contenidos%202024/Acceso%20abusivo%20a%20un%20sistema%20informatico%20y%20da%C3%B1o%20informatico.pdf

Colombia. Corte Suprema de Justicia (CSJ) (2022). *Sentencia SP592-2022* (Radicación n.º 50621; M. P. Diego Eugenio Corredor Beltrán). (https://cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1mar2022/SP592-2022(50621).pdf)

Colombia. Corte Suprema de Justicia (CSJ) (2022). *Sentencia SP2129-2022* (Radicación n.º 54153; M. P. Hugo Quintero Bernate). (https://cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1jul2022/SP2129-2022(54153).pdf)

Colombia. Corte Suprema de Justicia (CSJ) (2022). Sala de Casación Penal. *Sentencia SP2699-2022* (Rad. 59733). (https://cortesuprema.gov.co/corte/wp-content/uploads/relatorias/pe/b1ago2022/SP2699-2022(59733).pdf)

Colombia. Corte Suprema de Justicia (CSJ). (2023). *Sentencia SC037-2023* (M. P. Aroldo Wilson Quiroz Monsalvo). https://www.revistamisionjuridica.com/la-responsabilidad-objetiva-de-los-bancos-en-los-casos-de-fraude-electronico-en-colombia/

Cotrina Vidal, D. C., & Puentes Mora, C. M. (2018). Asignación indebida de competencia a los jueces penales municipales frente a los delitos informáticos. Universidad Militar Nueva Granada. https://repository.umng.edu.co/server/api/core/bitstreams/50bb2031-f44d-4c90-925f-c6df9cf44cdb/content

Council of Europe. (2001). *Convención sobre la delincuencia* [Convention on Cybercrime]. Budapest, Hungría. https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Cruz, E. P. (2025, February). Denuncias de ciberdelincuencia caen un 33% en Brasil. *Agência Brasil / EBC*. https://agenciabrasil.ebc.com.br/es/geral/noticia/2025-02/denuncias-de-ciberdelincuencia-caen-un-33-en-brasil#:~:text=Del%20total%2C%2052.999%20denuncias%20estuvieron

Cuenca Gonzaga, A. I., & Núñez Portilla, J. E. (s. f.). Análisis documental: impacto de la seguridad jurídica ante los delitos informáticos [Documentary analysis: impact of legal security in computer crime]. *LATAM Revista Latinoamericana de Ciencias Sociales y Humanidades, 5*(4), 2541–2551. https://latam.redilat.org/index.php/lt/article/view/2437/3063

De Oliveira, J. C. (2013). O cibercrime e as leis 12.735 e 12.737/2012. *Conteúdo Jurídico*. http://conteudojuridico.com.br/

De la Ossa Archila, M. F., & Corcione Morales, M. C. (2013). Prôtegis data. *Revista Digital de Derecho Administrativo, 10*, 111–143. https://revistas.uexternado.edu.co/index.php/Deradm/article/view/3688/3816

Delgado Granados, M. de L. (2010). *Delitos informáticos. Delitos electrónicos*. Orden Jurídico. https://www.ordenjuridico.gob.mx/Congreso/pdf/120.pdf

Díaz, R. M. (2022). *Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe*. CEPAL. https://repositorio.cepal.org/server/api/core/bitstreams/2b53c8ee-380e-47de-b115-298e8e06eeaa/content

Eilberg, D., et al. (2021, July 8). Os cuidados com a Convenção de Budapeste. *Jota*. https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/os-cuidados-com-a-convencao-de-budapeste-08072021

El Espectador. (2020, 4 de septiembre). *Google incumple 52 % de los requisitos de habeas data que exige Colombia: SIC*. https://www.elespectador.com/tecnologia/google-incumple-52-de-los-requisitos-de-habeas-data-que-exige-colombia-sic-article/

El Espectador. (2022, 22 de junio). *Credivalores recibe multimillonaria multa por el uso indebido de datos personales*. https://www.elespectador.com/economia/empresas/credivalores-recibe-multimillonaria-multa-por-el-uso-indebido-de-datos-personales/

El Tiempo (2021, 13 de noviembre). *Los detalles secretos del intento de secuestro de datos que sufrió el Dane. Director de la entidad descartó robo de datos, pues no había 'señales de salida'*

de la información. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/dane-asi-fue-el-intento-de-secuestro-de-datos-por-ciberataque-632163

Eslava-Zapata, R., García-Peñaloza, J. E., & Rojas-Hermida, C. J. (2023). Variables asociadas a los delitos informáticos en Latinoamérica. *Revista Academia & Derecho, 15*(28), 1–21. [Archivo local]

Espinoza Correa, C. P. (2014). Delitos informáticos y la Ley 19.223. *Actualidad Jurídica, (29)*, 553–565. https://derecho.udd.cl/actualidad-juridica/files/2021/01/AJ29_553.pdf

Estrada Garavilla, M. (2008). *Delitos informáticos*. https://perso.unifr.ch/derechopenal/assets/files/articulos/a_20080526_32.pdf

Fiscalía General de la Nación. (2025). *Informe de gestión 2024–2025*. https://www.fiscalia.gov.co/colombia/wp-content/uploads/Informe-de-Gestion-2024-2025.pdf

Fiscalía General de la Nación; Policía Nacional de Colombia. (2019). *Cartilla metodológica de atención de delitos informáticos*. Fiscalía General de la Nación. https://www.fiscalia.gov.co/colombia/wp-content/uploads/Cartilla-Metodologica-de-Atencion-de-Delitos-Informaticos.pdf

Flores Callejas, J., Afifi, A., & Lozinskiy, N. (2021). *La ciberseguridad en las organizaciones del sistema de las Naciones Unidas* (Informe de la Dependencia Común de Inspección). ONU. https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_spanish.pdf

Gamba Velandia, J. A. (2019). *El delito informático en el marco jurídico colombiano y el derecho comparado: Caso de la transferencia no consentida de activos* (Trabajo de grado). Universidad Externado de Colombia. https://bdigital.uexternado.edu.co/server/api/core/bitstreams/2e7e30f3-4a1f-45f6-b59a-dae6012b7210/content

Gamba, J. (2020). Panorama del derecho informático en América Latina y el Caribe. CEPAL. https://core.ac.uk/download/pdf/38672044.pdf

García Rico, J. C. (2023, Septiembre 14). Ciberataque en Colombia: Más grave y demorado de lo calculado. Miles de entidades que contaban con los servicios de IFX siguen fuera de línea y en apuros. *El Tiempo*. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberataque-en-colombia-es-mas-grave-y-demorado-de-lo-calculado-por-que-806234

Gobierno de Chile. (1993). *Ley n.º 19.223: Ley relativa a delitos informáticos* (sancionada 28 de mayo de 1993; Diario Oficial de la República de Chile, 7 de junio de 1993).

Gobierno de México. (2021). *Diagnóstico sobre delitos cibernéticos en la legislación penal del país*. https://estrategiasddhh.segob.gob.mx/work/models/EstrategiasDDHH/Documentos/pdf/GruposRiesgo/DIAGNOSTICO_DELITOS_CIBERNETICOS_ABRIL_2024_04-07-24.pdf

Gómez Pineda, V., Gómez Orozco, M. F., & Vidal Flórez, S. A. (2023). *Política criminal en la era digital: implicaciones y retos jurídicos del ciberterrorismo en Colombia*. Universidad CES. https://repository.ces.edu.co/server/api/core/bitstreams/9fa6f6dc-c62a-4a98-b5ef-ae775aec3c32/content

González Mama, M., & Chocano, F. (2025). *Brasil — Análisis de la constitucionalidad del artículo 19 del Marco Civil de Internet*. Universidad de Palermo. https://observatoriolegislativocele.com/wp-content/uploads/Informe-jurisprudencia-brasil-n%C2%B02.pdf

Guarnizo Portela, M. P. (2020). *La naturaleza jurídica de los delitos informáticos en Colombia* (Trabajo de grado). UNAD. https://repository.unad.edu.co/bitstream/handle/10596/41392/mpguarnizop.pdf?sequence=1

Guest, G., MacQueen, K. M., & Namey, E. E. (2012). *Applied thematic analysis*. Sage Publications. http://www.sagepub.com/books/Book233379

Gutiérrez, N. (2025). Estadísticas de ciberseguridad que debes conocer. *Preyproject*. https://preyproject.com/es/blog/estadisticas-seguridad-informatica

Herrera Avilés, H. P., Hidalgo Cajo, F. R., Ortega Campos, E. J., & Vallejo Lara, J. S. (2024). Una comparación de la tipificación del ciberdelito en Sudamérica. *Tesla, 4*(1). https://tesla.puertomaderoeditorial.com.ar/index.php/tesla/article/view/369/395

Herrera Peralta, M. E., López Ordóñez, S. M., & Rey Durán, C. A. (2018). *Análisis crítico de la Ley 1273 de 2009: Una lectura a partir de la perspectiva de su efectividad*. Universidad Cooperativa de Colombia. https://repository.ucc.edu.co/server/api/core/bitstreams/420c6e87-c9a4-472c-b09e-8bb63b11119c/content

Hertler, F. E. (2024). El convenio de Budapest y su influencia en el derecho penal argentino. *Revista de Pensamiento Penal, (500)*. https://www.pensamientopenal.com.ar/system/files/Documento_Editado1683.pdf

Higuera Arias, J. A. (2021). *Las debilidades en materia de protección de datos personales en la regulación emitida por el Estado colombiano*. Universidad Católica de Colombia. https://redcol.minciencias.gov.co/Record/UCATOLICA2_149148d840788647587c49b14f998332/Details

Infobae. (2018, May 13). Argentina se suma a la Convención de Budapest para tratar delitos informáticos. https://www.infobae.com/tecno/2018/05/13/argentina-se-suma-a-la-convencion-de-budapeste-para-tratar-delitos-informaticos/

Iriarte Ahon, E. (2005). *Estado situacional y perspectivas del derecho informático en América Latina y el Caribe*. CEPAL. https://repositorio.cepal.org/server/api/core/bitstreams/007ebbc8-9bd0-4e7d-9e27-ae41b75fa685/content

Japiassú, C. E. A., & Costa, R. de S. (2013). Informe de Brasil. *Coloquio Preparatorio, Sección IV. Derecho Penal Internacional*. https://www.penal.org/sites/default/files/files/RH%20-3.pdf

Jiménez Rozas, J. (2022). *Ciberdelincuencia: Evolución y relación con la actual situación de pandemia. Nuevas modalidades y nuevas problemáticas* (Tesis). Universidad de Salamanca. https://gredos.usal.es/bitstream/handle/10366/150144/TG_Jim%C3%A9nezRozas_Ciberdelincuencia.pdf?sequence=1&isAllowed=y

Kvale, S., & Brinkmann, S. (2015). *InterViews: Learning the craft of qualitative research interviewing* (3rd ed.). SAGE Publications.

Lara, J. C., Martínez, M., & Viollier, P. (2014). Hacia una regulación de los delitos informáticos basada en la evidencia. *Revista Chilena de Derecho y Tecnología*. http://www.derechoinformatico.uchile.cl/

Lavinder, K. (2016). Ataques cibernéticos: ¿Está preparada América Latina? *Air & Space Power Journal en Español, 28*(16), 39–45. https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-28_Issue-4/2016_4_05_lavinder_s.pdf

López Avella, J. P. (2014). *Criminalidad informática en Colombia* (Trabajo de grado). Universidad La Gran Colombia. https://repository.ugc.edu.co/server/api/core/bitstreams/3df12bb3-5c6b-44f7-a85e-c2f1a2a15598/content

López Avella, J. P. (2014). *Criminalidad informática en Colombia* (Trabajo de grado). Universidad La Gran Colombia. https://repository.ugc.edu.co/server/api/core/bitstreams/3df12bb3-5c6b-44f7-a85e-c2f1a2a15598/content

Loredo González, J. A., & Ramírez Granados, A. (2013). *Delitos informáticos: Su clasificación y una visión general de las medidas de acción para combatirlo*. Universidad Autónoma de Nuevo León. http://eprints.uanl.mx/3536/1/Delitos_informaticos.pdf

Manjarrés, I., & Jiménez, F. (2012). Caracterización de los delitos informáticos en Colombia. *Pensamiento Americano*, 71–82. https://dialnet.unirioja.es/descarga/articulo/8713900.pdf

Martínez-Vélez, J. A. (2022). *Hurto a través de medios informáticos y otras conductas delictivas semejantes en Colombia en 2022*. Universidad Católica de Colombia. https://repository.ucatolica.edu.co/server/api/core/bitstreams/e21a70d5-f51b-4c06-b5ea-47a50d3d8551/content

Martins dos Santos, B. (2022). *Convenio de Budapest sobre la ciberdelincuencia en América Latina: Un breve análisis sobre adhesión e implementación en Argentina, Brasil, Chile, Colombia y México*. Derechos Digitales. https://www.derechosdigitales.org/wp-content/uploads/ESP-Ciberdelincuencia-2022.pdf

Mediadefence. (2025). *Cibercrímenes – Latinoamérica*. https://www.mediadefence.org/resource-hub/cibercrimenes-latinoamerica/

Mesa Giraldo, M., & Ponce Jaramillo, L. F. (2023). La regulación de los delitos informáticos en Colombia: Logros y falencias en una sociedad de cibercriminalidad en auge. Universidad CES. https://repository.ces.edu.co/server/api/core/bitstreams/fedee197-db99-451c-9001-38bf3887ce7e/content

Ministerio de Justicia y Seguridad Pública (Brasil). (2021, December 16). Aprobada la adhesión de Brasil al Convenio de Budapest sobre la ciberdelincuencia. https://www.gov.br/mj/pt-br/assuntos/noticias/aprovada-adesao-do-brasil-a-convencao-de-budapeste-sobre-o-crime-cibernetico

Ministerio de la Presidencia de Costa Rica & Instituto Costarricense sobre Drogas. (2022). *Diagnóstico regional del estado del combate al lavado de activos derivado de los delitos cibernéticos en los países miembros de la OEA*. San José, Costa Rica. https://www.oas.org/es/sms/ddot/gelavex/53/docs/6-Diagn%C3%B3stico%20regional%20lavado%20y%20delitos%20cibern%C3%A9ticos.pdf

Ministerio de la Presidencia de Costa Rica & Instituto Costarricense sobre Drogas. (2022). Informe sobre ciberdelincuencia en Brasil. [Citado en Martins dos Santos, 2022, pp. 9–10]. *(Si deseas, puedo localizar el documento original y formatearlo plenamente.)*

Narváez Montenegro, B. D., & Recalde Machado, G. E. (2018). El delito informático en América. *Debate Jurídico Ecuador, 1*(1), 3–14. https://revista.uniandes.edu.ec/ojs/index.php/DJE/article/download/1206/602

Narváez Montenegro, D. B. (2015). El delito informático y su clasificación. *Episteme. Revista digital de ciencia, tecnología e innovación, 2*(2), 158–173. https://www.redalyc.org/pdf/5646/564660011007.pdf

Navarro Ramírez, A. C., & Díaz Serrato, Y. M. (2024). *Los delitos informáticos dentro del sistema penal vigente en Colombia*. Universidad de Ibagué. https://repositorio.unibague.edu.co/server/api/core/bitstreams/cb3f045d-a2ae-44da-914b-78a0a3e45caa/content

Navarro, R. (2003). El concepto de delito informático según la nueva legislación chilena (Ley n.º 21.459). *Política Criminal*. http://politcrim.com/wp-content/uploads/2023/12/Vol18N36A7.pdf

Negro, E. N. (2023). Fintech: Entre la inclusión financiera y el cibercrimen. *Revista Jurídica de San Isidro, Núm. II*. https://www.casi.com.ar/sites/default/files/2023-09/I-Negro.pdf

Newton, C. (2024). Secuestrar datos para pedir rescate es un negocio en auge en Brasil. *InsightCrime*. https://insightcrime.org/es/noticias/secuestrar-datos-negocio-auge-brasil/

Ojeda, D. (2024, Agosto 21). Colombia en la mira: Se registran más de 118 ataques cibernéticos por minuto. *El Espectador.* https://www.elespectador.com/tecnologia/colombia-en-la-mira-se-registran-mas-de-118-ataques-ciberneticos-por-minuto/

Organización de las Naciones Unidas (ONU). (2010a). Resolución aprobada por la Asamblea General [A/55/L.2]. Nueva York: ONU. https://docs.un.org/es/A/RES/55/2

Organización de las Naciones Unidas (ONU). (2010b). Resolución aprobada por la Asamblea General el 21 de diciembre de 2010 [A/65/457]. Nueva York: ONU. https://docs.un.org/es/A/RES/65/230

Organización de las Naciones Unidas (ONU). (2010c). *12.º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, Salvador (Brasil), 12–19 de abril de 2010* (A/CONF.213/L.6/Rev.2). Nueva York: ONU. https://docs.un.org/es/A/CONF.213/L.6/REV.2

Organización de las Naciones Unidas (ONU). (2024). *Lucha contra la utilización de las tecnologías de la información y las comunicaciones con fines delictivos: Informe de la Tercera Comisión, relatora Sra. Robin de Vogel (A/79/460)*. Nueva York: ONU. https://docs.un.org/es/A/79/460

Organización de los Estados Americanos (OEA) & Trend Micro. (2013). *Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos*. Washington, DC: OEA & Trend Micro. https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2013%20-%20Tendencias%20en%20la%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe%20y%20Respuestas%20de%20los%20Gobiernos.pdf

Organización de los Estados Americanos (OEA). (2013). *Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos*. Washington, DC: OEA. https://www.oas.org/es/sms/cicte/ciberseguridad/publicaciones/2013%20-%20Tendencias%20en%20la%20Seguridad%20Cibern%C3%A9tica%20en%20Am%C3%A9rica%20Latina%20y%20el%20Caribe%20y%20Respuestas%20de%20los%20Gobiernos.pdf

Palazuelos Covarrubias, I. (2023). Ciberseguridad y ciberdelincuencia: regulación vigente y pendientes legislativos en materia de robo de identidad y fraude. *Quórum Legislativo, 142*, 75–105. https://revistas-colaboracion.juridicas.unam.mx/index.php/quorum/article/viewFile/41916/38664

Parra, J. W. (2024). *Determinar la eficacia de la Ley 1273, entre el año 2010–2022 en el departamento de Risaralda* (Trabajo de grado). Universidad Cooperativa de Colombia. https://repository.ucc.edu.co/server/api/core/bitstreams/2fbc06d2-f269-4d03-83bd-f0130ad04159/content

Patton, M. Q. (2015). *Qualitative research & evaluation methods: Integrating theory and practice* (4th ed.). SAGE Publications.

Penna, N. S., Gamero, N., Micelotta, M. J., & Di Pasquasio, F. G. (2022). Evolución del phishing en Argentina. En M. Fernández, M. Césari & G. Martínez (Eds.), *9° Congreso Nacional de Ingeniería Informática/Sistemas de Información CONAIISI — Memoria de trabajos*. Universidad Tecnológica Nacional. (Material suministrado).

Peña Peña, M. E. (2023). *Delitos cibernéticos* (Trabajo de grado). Universidad Libre de Colombia. https://repository.unilibre.edu.co/bitstream/handle/10901/24774/TESIS%20VERSION%20APROBADA.pdf?sequence=1&isAllowed=y

Peralis Security. (s. f.). Brasil, ¿el país del cibercrimen? Un panorama del escenario actual. https://www.perallis.com/noticias/brasil-el-pais-del-cibercrimen-un-panorama-del-escenario-actual#:~:text=Los%20ataques%20cibern%C3%A9ticos%20representan%20riesgos,una%20nueva%20cuenta%20por%20minuto!

Pilmayquén Reina, I. (2013). *Delitos informáticos en Latinoamérica. Estudio de sus legislaciones*. Universidad de Buenos Aires. https://www.pensamientopenal.com.ar/system/files/2015/03/doctrina40720.pdf

Posada Maya, R. (2006). Aproximación a la criminalidad informática en Colombia. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías, 2*, 11–60. https://dialnet.unirioja.es/servlet/oaiart?codigo=7510293

Presidencia de la Nación (Argentina). (2018). *Ley n.º 27.411: Convenio sobre ciberdelito del Consejo de Europa*. https://www.argentina.gob.ar/normativa/nacional/ley-27411-304798

Presidencia de la República (Diário Oficial). (2012, 30 de noviembre). *Lei n.º 12.737/2012* (tipificación de delitos informáticos). http://planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm

Presidencia de la República de Brasil. (2014). *Lei n.º 12.965, de 23 de abril de 2014: Marco Civil da Internet*. http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

Presidencia de la República de Brasil. (2018). *Lei n.º 13.709, de 14 de agosto de 2018: Lei Geral de Proteção de Dados Pessoais (LGPD)*. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Reyes Cuartas, J. F. (2007). El delito informático en Colombia: insuficiencias regulativas. *Derecho Penal y Criminología, 28*, 101–118. https://revistas.uexternado.edu.co/index.php/derpen/article/view/963/913

Rincón Arteaga, J. A., Castiblanco Hernández, S. A., Quijano Díaz, A., Urquijo Vanegas, J. D., & Pregonero León, Y. K. (2022). Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la ley de delitos informáticos? *Revista Criminalidad, 64*(3), 95–116. https://doi.org/10.47741/17943108.368

Rodrigues, G. (2021, noviembre). A Convenção de Budapeste sobre o cibercrime e as controvérsias sobre a adesão brasileira. Instituto de Referência em Internet e Sociedade (IRIS). https://irisbh.com.br/a-convencao-de-budapeste-sobre-o-cibercrime-e-as-controversias-sobre-a-adesao-brasileira/

Rodríguez, M., Barrios, P., & Fuentes, L. (1984). *Derecho penal y tecnología*. Editorial Jurídica.

Roesener, A. G. (2015). Política para la seguridad cibernética de EUA. *Air & Space Power Journal, 2*(11), 73–83. https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-27_Issue-2/2015_2_11_roesener_s.pdf

Roesener, A. G. (2015). Política para la seguridad cibernética de EUA. *Air & Space Power Journal, 2*(11), 73–83. https://www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-27_Issue-2/2015_2_11_roesener_s.pdf

Romero Silvera, G. (2010). *Interés público y protección de datos personales*. Seminario Regional de Protección de Datos. https://www.redipd.org/sites/default/files/2020-01/Graciela_Romero.pdf

SaferNet Brasil / Afernet Brasil. (s. f.). *PL sobre crimes cibernéticos: Projeto de Lei Substitutivo do Senador Eduardo Azeredo (PSDB-MG)*. https://www.safernet.org.br/site/institucional/projetos/obsleg/pl-azeredo

Sánchez Castillo, Z. N. (2017). *Análisis de la Ley 1273 de 2009 y la evolución de la ley con relación a los delitos informáticos en Colombia* (Trabajo de grado). Universidad Nacional Abierta y a Distancia (UNAD). https://repository.unad.edu.co/bitstream/handle/10596/11943/1053323761.pdf?sequence=1

Sánchez Castillo, Z. N. (2017). *Análisis de la Ley 1273 de 2009 y la evolución de la Ley con relación a los delitos informáticos en Colombia* (Trabajo de grado). Universidad Nacional Abierta y a Distancia (UNAD). https://repository.unad.edu.co/bitstream/handle/10596/11943/1053323761.pdf?sequence=1

Schurjin. (2022). [Análisis sobre legislación argentina en materia de delitos informáticos y modificaciones al art. 128 y ley 27.436] (Extracto suministrado). *(Extracto suministrado por el usuario).*

Seger, A. (2016). El estado actual de la legislación sobre el delito cibernético en América Latina y el Caribe: Algunas observaciones. En *Informe Ciberseguridad 2016* (pp. 19–23). Organización de los Estados Americanos & Banco Interamericano de Desarrollo. https://publications.iadb.org/publications/spanish/document/Ciberseguridad-%C2%BFEstamos-preparados-en-Am%C3%A9rica-Latina-y-el-Caribe.pdf

Senado Federal (Brasil). (2021). *Projeto de Decreto Legislativo n.º 255 de 2021 / Decreto Legislativo n.º 37 de 2021 (aprovação do texto do Convenio de Budapeste)*. https://www25.senado.leg.br/web/atividade/materias/-/materia/150258

SEON. (2022). *Informe global sobre ciberdelincuencia: ¿Qué países corren mayor riesgo?* https://seon.io/es/recursos/informe-global-sobre-ciberdelincuencia-que-paises-corren-mayor-riesgo/

Serrano Buitrago, E. R. (2014). *La práctica de delitos informáticos en Colombia* (Trabajo de grado). Universidad La Gran Colombia. https://repository.umng.edu.co/server/api/core/bitstreams/d3b0b7dd-b9af-44ab-a94d-c1e0ce0c1533/content

Serrano Buitrago, E. R. (2014). *La práctica de delitos informáticos en Colombia* (Trabajo de grado). Universidad Militar Nueva Granada. https://repository.umng.edu.co/server/api/core/bitstreams/d3b0b7dd-b9af-44ab-a94d-c1e0ce0c1533/content

Supremo Tribunal Federal (STF). (2020). *Audiencia pública n.º 29 (transcripciones)*. http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/ADC51Transcricoes.pdf

Supremo Tribunal Federal (STF). (s. f.). *ADC 51 (detalle del incidente)*. http://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379

Temperini, M. G. I. (2014a). *Delitos informáticos en Latinoamérica: Un estudio de derecho comparado* (1ª parte). Universidad Nacional del Litoral. https://www.academia.edu/33134232/Delitos_Informaticos_en_Latinoamerica

Temperini, M. G. I. (2014b). *Delitos informáticos en Latinoamérica: Un estudio de derecho comparado* (2ª parte). XIV Simposio Argentino de Informática y Derecho (SID). https://43jaiio.sadio.org.ar/proceedings/SID/13.pdf

Terán Villafuerte, B. J. (2022). *Análisis de delitos informáticos relevantes en organizaciones gubernamentales en América Latina* (Trabajo de grado). Universidad Politécnica Salesiana. https://dspace.ups.edu.ec/bitstream/123456789/24407/4/UPS-GT004244.pdf

Unión Internacional de Telecomunicaciones (ITU). (2009). *El ciberdelito: Guía para los países en desarrollo*. Ginebra, Suiza. https://www.itu.int/dms_pub/itu-d/oth/01/0b/d010b0000073301pdfs.pdf

UNIR. (2025). ¿Qué tipos de delitos informáticos existen? Claves y legislación en Colombia. https://colombia.unir.net/actualidad-unir/tipos-delitos-informaticos/

Universidad Externado de Colombia. (2016). *Ciberseguridad: ¿Cómo está Latinoamérica y el Caribe?* Blog de Derecho de los Negocios. https://dernegocios.uexternado.edu.co/comercio-electronico/ciberseguridad-como-esta-latinoamerica-y-el-caribe/

UNODC. (2013). *Estudio exhaustivo del problema del delito cibernético y las respuestas de los Estados Miembros, la comunidad internacional y el sector privado ante ese fenómeno*. Viena: UNODC. https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_S.pdf

UNODC. (2021). *Estados Unidos de América (submission / documents sobre cibercrimen)*. Viena, Austria. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/2021_1026_US_National_Submission_AHC_-_S.pdf

Vallejo Lara, J. S., Herrera Avilés, H. P., Ortega Campos, E. J., & Hidalgo Cajo, F. R. (2024). Una comparación de la tipificación del ciberdelito en Sudamérica. *Tesla Revista Científica, 4*(1). https://tesla.puertomaderoeditorial.com.ar/index.php/tesla/article/view/369/395

Vásquez Vélez, A. (2021). *El ámbito de aplicación del régimen jurídico colombiano para la protección de datos personales. Su alcance frente a empresas extranjeras sin representación jurídica en Colombia*. Pontificia Universidad Javeriana. https://apidspace.javeriana.edu.co/server/api/core/bitstreams/0fec4082-7ea5-472c-be4e-dbe2da8dddf1/content

Victoria, M. A. A., & Delgado Arango, D. F. (2018). *Eficacia normativa sobre los delitos informáticos en Colombia*. Universidad Libre. https://repository.unilibre.edu.co/bitstream/handle/10901/26654/EFICACIA%20NORMATIVA%20SOBRE%20LOS%20DELITOS%20INFORM%C3%81TICOS%20EN%20COLOMBIA%20PDF.pdf?sequence=1&isAllowed=y

Yin, R. K. (2019). *Case study research and applications: Design and methods* (6th ed.). Sage Publications.