REVISTA MULTIDISCIPLINAR EPISTEMOLOGÍA DE LAS CIENCIAS

Volumen 3, Número 1
Enero-Marzo 2026

Edición Trimestral

CROSSREF PREFIX DOI: 10.71112

ISSN: 3061-7812, www.omniscens.com

Revista Multidisciplinar Epistemología de las Ciencias

Volumen 3, Número 1
enero-marzo 2026

Publicación trimestral
Hecho en México

La Revista Multidisciplinar Epistemología de las Ciencias acepta publicaciones de cualquier área del conocimiento, promoviendo una plataforma inclusiva para la discusión y análisis de los fundamentos epistemológicos en diversas disciplinas. La revista invita a investigadores y profesionales de campos como las ciencias naturales, sociales, humanísticas, tecnológicas y de la salud, entre otros, a contribuir con artículos originales, revisiones, estudios de caso y ensayos teóricos. Con su enfoque multidisciplinario, busca fomentar el diálogo y la reflexión sobre las metodologías, teorías y prácticas que sustentan el avance del conocimiento científico en todas las áreas.

Contacto principal: admin@omniscens.com

9773061781003

Cintillo legal

Revista Multidisciplinar Epistemología de las Ciencias Vol. 3, Núm. 1, enero-marzo 2026, es una publicación trimestral editada por el Dr. Moises Ake Uc, C. 51 #221 x 16B , Las Brisas, Mérida, Yucatán, México, C.P. 97144 , Tel. 9993556027, Web: https://www.omniscens.com, admin@omniscens.com, Editor responsable: Dr. Moises Ake Uc. Reserva de Derechos al Uso Exclusivo No. 04-2024-121717181700-102, ISSN: 3061-7812, ambos otorgados por el Instituto Nacional del Derecho de Autor (INDAUTOR). Responsable de la última actualización de este número, Dr. Moises Ake Uc, fecha de última modificación, 1 enero 2026.

Revista Multidisciplinar Epistemología de las Ciencias

Volumen 3, Número 1, 2026, enero-marzo

DOI: https://doi.org/10.71112/d3625c91

LA CIBERCRIMINALIDAD EN MÉXICO: ENTRE LA DISPERSIÓN NORMATIVA Y LA IMPUNIDAD DIGITAL

CYBERCRIME IN MEXICO: BETWEEN NORMATIVE FRAGMENTATION AND DIGITAL IMPUNITY

Luis Alfonso Gala Rodríguez

México

DOI: https://doi.org/10.71112/d3625c91

La cibercriminalidad en México: entre la dispersión normativa y la impunidad digital

Cybercrime in Mexico: between normative fragmentation and digital impunity

Luis Alfonso Gala Rodríguez

p.luisgala@gmail.com

https://orcid.org/0009-0004-8891-8445

Centro de Estudios Superiores en Ciencias Jurídicas y Criminológicas

México

RESUMEN

La cibercriminalidad en México constituye uno de los desafíos más complejos para el derecho penal contemporáneo. A pesar del incremento sostenido de los delitos informáticos, la respuesta jurídica mexicana evidencia dispersión normativa, falta de tipificación uniforme y debilidad institucional en su persecución. El presente estudio, desde una perspectiva dogmática y crítica, analiza el marco penal federal vigente, su insuficiencia frente a la dinámica digital y la necesidad de una política criminal coherente que armonice los principios del derecho penal con la realidad tecnológica. Se realiza un ejercicio de derecho comparado con sistemas europeos y latinoamericanos, para identificar criterios de eficacia legislativa y posibles rutas de adecuación normativa para México.

Palabras clave: derecho penal digital; ciberdelincuencia; política criminal; impunidad; dispersión normativa; tipificación penal; derecho comparado; ciberseguridad; responsabilidad penal

DOI: https://doi.org/10.71112/d3625c91

ABSTRACT

Cybercrime in Mexico represents one of the most complex challenges for contemporary criminal law. Despite the steady increase in computer-related offenses, the Mexican legal response reveals regulatory dispersion, lack of uniform typification, and institutional weaknesses in prosecution. From a dogmatic and critical approach, this study analyzes the current federal criminal framework, its inadequacies in addressing digital dynamics, and the need for a coherent criminal policy aligning penal principles with technological realities. A comparative law analysis with European and Latin American systems is conducted to identify legislative efficiency criteria and potential pathways for Mexico's normative harmonization.

Keywords: cybercrime regulation; digital criminal law; normative fragmentation; digital impunity; criminal policy

Recibido: 30 diciembre 2025 | Aceptado: 14 enero 2026 | Publicado: 15 enero 2026

INTRODUCCIÓN

La ciberdelincuencia se ha consolidado como uno de los fenómenos criminales más complejos y dinámicos del siglo XXI, caracterizándose por su capacidad de trascender fronteras territoriales, desdibujar jurisdicciones tradicionales y desafiar los modelos clásicos de imputación penal. En el contexto mexicano, este fenómeno revela con particular claridad la tensión permanente entre la acelerada evolución tecnológica y la limitada capacidad del derecho penal para adaptarse de manera sistemática y coherente a nuevas formas de criminalidad digital (Aguirre Quezada, 2022).

Diversos estudios coinciden en señalar que México enfrenta un escenario de rezago normativo estructural en materia de ciberdelincuencia, lo que se traduce en altos niveles de impunidad y en una tutela deficiente de bienes jurídicos fundamentales como la privacidad, la

seguridad de la información y el patrimonio digital (Alcalá Casillas, 2024; Palazuelos Covarrubias, 2023). Esta situación se agrava por la ausencia de una política criminal integral en materia de ciberseguridad, así como por la falta de armonización legislativa entre los distintos niveles de gobierno.

Este fenómeno no es exclusivo del contexto mexicano, sino que se inscribe en una dinámica regional caracterizada por el incremento sostenido de los delitos informáticos y por respuestas estatales fragmentadas e insuficientes. En el ámbito latinoamericano, diversos estudios han identificado variables estructurales asociadas a la expansión de la cibercriminalidad, entre ellas la debilidad institucional, la dispersión normativa y la limitada capacidad de adaptación de los sistemas penales frente a la innovación tecnológica (Eslava Zapata et al., 2024). En el caso de México, estas condiciones se manifiestan de forma particularmente aguda, profundizando escenarios de impunidad digital y afectando la tutela efectiva de bienes jurídicos fundamentales (Aguirre Quezada, 2022; Alcalá Casillas, 2024).

El Código Penal Federal, si bien ha sido objeto de reformas parciales para incorporar algunas figuras relacionadas con el acceso ilícito a sistemas informáticos y la alteración de datos, continúa ofreciendo una regulación fragmentaria y limitada frente a la diversidad de conductas que hoy integran la criminalidad digital. A partir del análisis doctrinal y normativo, puede sostenerse que el legislador mexicano ha respondido a la ciberdelincuencia mediante reformas parciales y sectoriales, sin desarrollar una dogmática penal integral que sistematice los delitos informáticos como una categoría autónoma de protección penal, fenómeno que ya había sido advertido, en términos generales, por (Cassou Ruiz, 2009) al señalar la fragmentación y debilidad conceptual de la regulación existente.

A esta falta sistémica en la regulación sustantiva se suma un problema estructural de mayor magnitud: el policentrismo legislativo o la fragmentación normativa. En el marco jurídico mexicano actual, las disposiciones penales y aquellas con efectos cuasipenales que se refieren

al comportamiento delictivo en entornos digitales están distribuidas en una variedad de instrumentos jurídicos especializados. Algunos de los más importantes son la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, el grupo de regulaciones financieras, los paquetes reformadores recientes que se conocen como "Ley Olimpia", y las diversas clasificaciones presentes en los códigos penales de las 32 entidades federativas.

En ausencia de un eje de coordinación dogmático-técnico, se produce esta dispersión, que genera serias deficiencias en tres aspectos esenciales del sistema penal: la certeza jurídica (para los ciudadanos y los operadores jurídicos), la eficacia procesal (en la investigación y persecución de delitos) y la coherencia interna (evitando vacíos y contradicciones). Como señala (Alcalá Casillas, 2024), la regulación de la cibercriminalidad en México se caracteriza por una fragmentación normativa significativa, resultado de la coexistencia desarticulada de regímenes federales, estatales y especiales que no tienen criterios comunes para armonizar dogmáticamente ni técnicas legislativas comunes que faciliten una respuesta penal integrada y equilibrada.

El presente estudio persigue dos objetivos principales. En primer lugar, examinar críticamente el marco jurídico penal federal mexicano frente a los delitos informáticos, identificando los factores normativos, dogmáticos e institucionales que contribuyen a su dispersión y debilidad estructural. En segundo término, proponer, desde el derecho comparado, modelos de armonización normativa que permitan fortalecer la eficacia del sistema penal mexicano frente a la ciberdelincuencia, sin sacrificar los principios de legalidad, proporcionalidad e intervención mínima.

Marco teórico

El análisis de la cibercriminalidad desde el derecho penal contemporáneo exige una aproximación dogmática que permita delimitar los alcances legítimos de la intervención punitiva

del Estado en contextos tecnológicos complejos. En este sentido, la presente investigación se inscribe en la tradición del derecho penal garantista, conforme a la cual el ejercicio del *ius puniendi* debe observar estrictamente los principios de legalidad, proporcionalidad e intervención mínima, evitando respuestas expansivas o meramente simbólicas frente a fenómenos sociales emergentes.

Desde esta perspectiva, el derecho penal se concibe como un instrumento de última ratio, orientado prioritariamente a la protección de bienes jurídicos esenciales cuando otros mecanismos de control jurídico resultan insuficientes. En el entorno digital, esta función adquiere especial relevancia, dado que las conductas desplegadas en el ciberespacio pueden generar afectaciones de gran intensidad y persistencia sobre derechos fundamentales como la intimidad, la integridad psíquica, la libertad sexual y el patrimonio, cuya vulneración se ve amplificada por la escala, velocidad y permanencia propias de las tecnologías de la información.

La doctrina penal contemporánea ha advertido que la criminalidad digital plantea desafíos sustantivos a las categorías clásicas del derecho penal, particularmente en lo relativo a la delimitación de la tipicidad, la identificación del bien jurídico protegido y la configuración de la relación de causalidad en entornos desmaterializados. No obstante, estos desafíos no justifican un abandono de los principios garantistas, sino que exigen una adaptación dogmática rigurosa, capaz de ofrecer respuestas normativas eficaces sin incurrir en inflaciones penales o en la criminalización excesiva de conductas que pueden ser atendidas por otras ramas del ordenamiento jurídico.

La persistencia de estos desafíos confirma que la problemática de la cibercriminalidad no puede abordarse únicamente desde una perspectiva normativa reactiva, sino que exige una revisión crítica de la dogmática penal tradicional. Ya desde etapas tempranas de la regulación mexicana, la doctrina advertía la falta de sistematicidad conceptual en materia de delitos

informáticos (Cassou Ruiz, 2009), déficit que hoy se ve agravado por la incorporación de tecnologías emergentes como la inteligencia artificial y los sistemas automatizados de decisión.

En este contexto, los estudios comparados en América Latina evidencian la necesidad de reconstruir categorías como autoría, imputación y responsabilidad penal frente a escenarios de mediación algorítmica y autonomía tecnológica, sin renunciar a los principios garantistas que informan el derecho penal contemporáneo(Alé Martínez & Aguilar Campos, 2025; Maculan et al., 2024).

En el plano internacional, el Convenio de Budapest sobre la Ciberdelincuencia constituye el principal referente teórico-normativo en materia de regulación penal de los delitos informáticos, al establecer estándares mínimos de tipificación y mecanismos de cooperación transnacional frente a fenómenos delictivos de naturaleza global (Consejo de Europa, 2001).

La relevancia de este instrumento se ha visto reforzada con la adopción de su Segundo Protocolo Adicional, orientado a fortalecer la cooperación internacional y la obtención de pruebas electrónicas en investigaciones penales (Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y La revelación de pruebas electrónicas, 2023).

A este escenario normativo se suma la reciente adopción de la Convención de las Naciones Unidas contra la Ciberdelincuencia, la cual busca establecer un marco global de cooperación penal frente a delitos informáticos, ampliando el espectro de obligaciones estatales en materia de investigación, intercambio de información y asistencia jurídica internacional(Naciones Unidas, 2025).

La coexistencia de este nuevo instrumento con el Convenio de Budapest plantea desafíos relevantes para los Estados que aún no han adherido a este último, como México, al tiempo que reabre el debate sobre la armonización normativa, la soberanía penal y la

protección de derechos fundamentales en el contexto de la cooperación transnacional (Centeno, 2018; Consejo de Europa, 2025).

El debate en torno a la eventual adhesión de México al Convenio de Budapest ha puesto de relieve tensiones entre la necesidad de armonización normativa y las exigencias del orden constitucional interno. Mientras algunos sectores han advertido posibles riesgos para la soberanía y los derechos fundamentales (Centeno, 2018), estudios recientes del Poder Legislativo destacan los beneficios del instrumento en términos de estandarización normativa, cooperación internacional y fortalecimiento de las capacidades institucionales frente a la criminalidad digital (Cámara de Diputados LXV Legislatura, 2023; Consejo de Europa, 2025), a pesar de ello, hasta la publicación del presente artículo, México no ha firmado la Adhesión al Convenio sobre Ciberdelincuencia.

Desde una perspectiva teórica, el análisis comparado muestra que los modelos normativos más avanzados en materia de ciberdelincuencia se caracterizan por una mayor coherencia sistemática y por la incorporación de tipos penales específicos que atienden las particularidades del entorno digital. En este sentido, la experiencia de países como España y Argentina refleja una tendencia hacia la especialización normativa y la alineación con los estándares internacionales, sin renunciar a los principios fundamentales del derecho penal (Ley 26.388, 2008; Ley Orgánica 1/2015, 2015).

En contraste, la doctrina nacional ha señalado que el ordenamiento jurídico mexicano presenta un déficit estructural en su política criminal digital, derivado de la dispersión normativa, la ambigüedad dogmática y las debilidades institucionales en la persecución penal de los delitos informáticos (Aguirre Quezada, 2022; Alcalá Casillas, 2024). Este contexto refuerza la necesidad de un marco teórico que permita analizar críticamente la regulación penal vigente y evaluar su compatibilidad con un modelo de derecho penal garantista, capaz de responder

eficazmente a los riesgos del ciberespacio sin comprometer la tutela de los derechos fundamentales.

METODOLOGÍA

La investigación se desarrolló mediante un enfoque cualitativo, con un diseño documental, no experimental y analítico, sustentado en el método jurídico-dogmático y crítico. El estudio se orientó al análisis sistemático del marco penal mexicano aplicable a la cibercriminalidad, así como de la doctrina especializada, con el propósito de identificar las causas normativas e institucionales de su fragmentación y su impacto en la eficacia del sistema penal.

De manera complementaria, se empleó el método comparado, contrastando el modelo mexicano con experiencias normativas de España, Argentina y Chile, así como con los estándares del Convenio de Budapest sobre la Ciberdelincuencia, a fin de identificar criterios de armonización normativa y buenas prácticas legislativas.

La búsqueda y selección del corpus documental se realizó mediante consulta en bases de datos académicas especializadas en ciencias jurídicas y sociales, como SciELO (Scientific Electronic Library Online), Dialnet, Redalyc, DOAJ (Directory of Open Access Journals) y HeinOnline, así como en repositorios institucionales oficiales como los de la Cámara de Diputados de México, el Instituto Nacional de Estadística y Geografía (INEGI), el Consejo de Europa y los portales legislativos de España, Argentina y Chile. Se emplearon combinaciones de términos clave en español e inglés (“ciberdelincuencia”, “derecho penal digital”, “cybercrime”, “Budapest Convention”, “México”) y se aplicaron filtros por relevancia temática y vigencia temporal (documentos publicados desde 2008 hasta 2025 en razón de su importancia y actualidad en relación al tema de estudio. Asimismo, se incorporaron datos estadísticos oficiales del INEGI para contextualizar la respuesta institucional frente a la cibercriminalidad. El

análisis se realizó mediante sistematización normativa, evaluación dogmática y contraste comparado de los resultados.

La definición de las variables analíticas, la clasificación de los incidentes cibernéticos y la delimitación de las capacidades institucionales consideradas en el análisis empírico se sustentaron en el diseño metodológico del Censo Nacional de Seguridad Pública Federal y Estatal, particularmente en lo relativo a los criterios de levantamiento, sistematización y presentación de la información estadística oficial (INEGI, 2025a). Esta referencia metodológica permitió asegurar la coherencia entre los datos analizados y los estándares técnicos empleados por la autoridad estadística nacional.

RESULTADOS

Los resultados derivados del análisis normativo, doctrinal y empírico permiten identificar un panorama caracterizado por la fragmentación normativa, la insuficiencia dogmática y la limitada eficacia institucional de la respuesta penal mexicana frente a la cibercriminalidad. Los hallazgos se organizan en cuatro ejes analíticos: 1) marco normativo penal, 2) tipificación de conductas, 3) eficacia institucional y 4) derecho comparado y propuestas de armonización.

1. Marco normativo penal mexicano: una arquitectura fragmentada.

El examen del Código Penal Federal (CPF) evidencia que el ordenamiento penal mexicano carece de una regulación sistemática y autónoma de la ciberdelincuencia. No existe un título, capítulo o sección específica dedicada a los delitos informáticos, lo que obliga a interpretar disposiciones dispersas en distintos apartados del código.

En particular, los artículos 211 Bis y subsecuentes —incorporados originalmente en 1999 y reformados de manera puntual en años posteriores— tipifican conductas relacionadas con el acceso no autorizado a sistemas informáticos, la interferencia y el aprovechamiento indebido de información (Código Penal Federal (CPF), 2025). Sin embargo, su formulación

presenta deficiencias técnicas y conceptuales, lo que genera problemas de interpretación y aplicación práctica.

A esta insuficiencia estructural se suma la proliferación de leyes especiales de carácter reactivo, que introducen disposiciones penales o cuasipenales vinculadas con conductas digitales sin integrarse en una política criminal coherente.

Un ejemplo paradigmático es el conjunto de reformas conocido como Ley Olimpia, mediante el cual se adicionaron disposiciones a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y al propio CPF para reconocer y sancionar la violencia digital y la vulneración de la intimidad sexual a través de medios tecnológicos (Decreto por el que se adicionan diversas disposiciones a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y al Código Penal Federal (Ley Olimpia), 2021). Si bien estas reformas representan un avance en la tutela de derechos específicos, su incorporación se realizó sin una articulación dogmática integral con el resto del sistema penal.

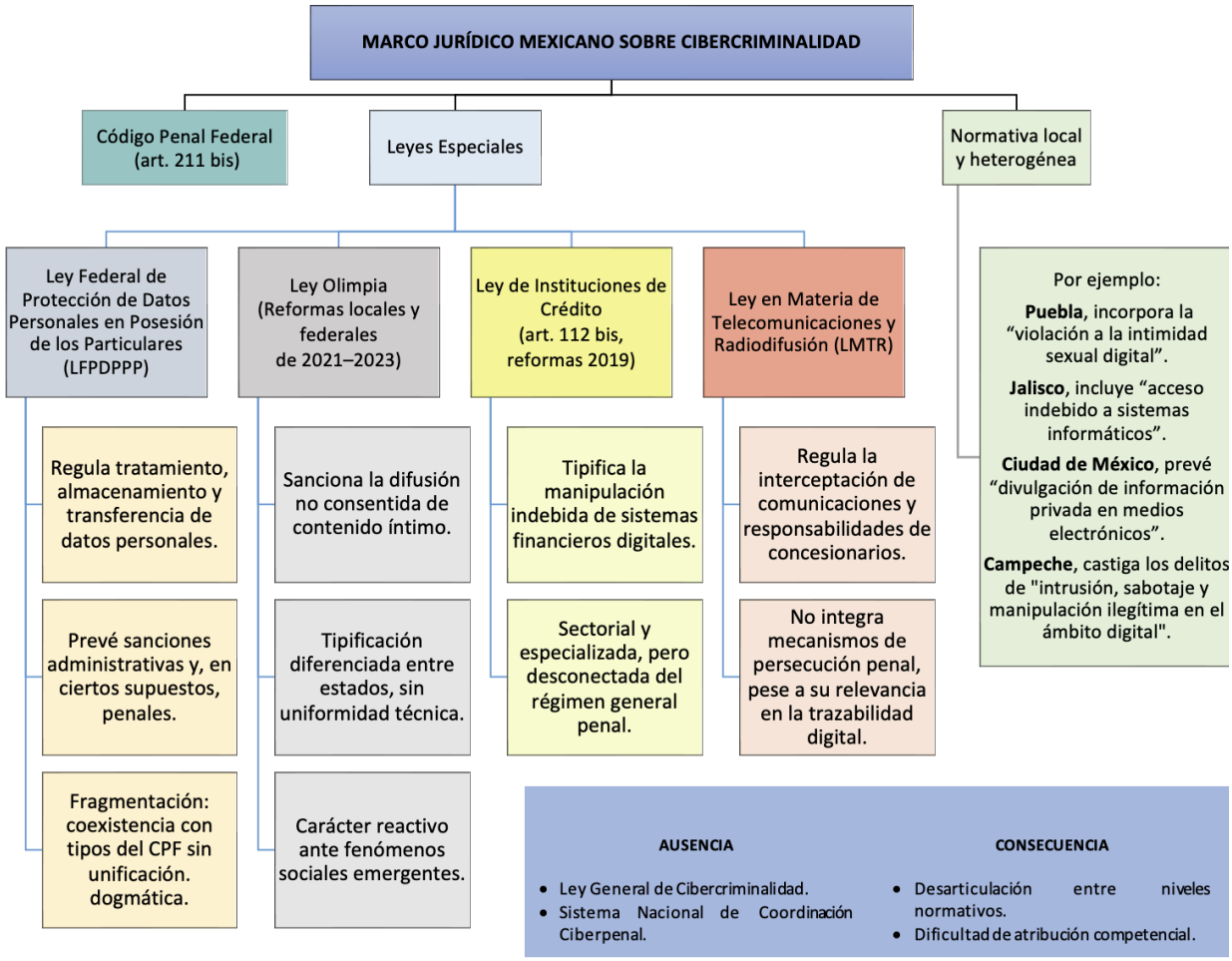
De forma similar, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares combina mecanismos administrativos y penales para sancionar el tratamiento indebido de datos, generando zonas de solapamiento normativo y criterios sancionadores divergentes (Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPP), 2010).

Como señalan Alcalá Casillas & Meléndez Ehrenzweig (2023), la coexistencia de normas federales, estatales y administrativas sin coordinación sistemática produce inseguridad jurídica y debilita la eficacia de la persecución penal.

Figura 1

Dispersión normativa mexicana en materia de cibercriminalidad.

DOI: https://doi.org/10.71112/d3625c91



Fuente: elaboración propia con base en el Código Penal Federal, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Ley Olimpia, Ley de Instituciones de Crédito, Ley en Materia de Telecomunicaciones y Radiodifusión, y legislaciones estatales (Códigos Penales de: Puebla, Jalisco, CDMX, Campeche).

Este esquema ilustra que el marco jurídico mexicano carece de una estructura sistemática unificada para abordar la cibercriminalidad. La coexistencia de normas penales, administrativas y locales sin articulación dogmática compromete la aplicación del principio de legalidad y la eficacia procesal. A diferencia de los modelos europeos o sudamericanos —que han consolidado leyes integrales de ciberdelincuencia—, México mantiene una arquitectura fragmentada que responde de manera reactiva y parcial a fenómenos digitales emergentes.

Este diseño normativo fragmentado compromete principios básicos del derecho penal, en particular el principio de legalidad en su vertiente de *lex certa*, al dificultar que los destinatarios de la norma y los operadores jurídicos identifiquen con claridad el alcance de las conductas prohibidas. En contraste con ordenamientos que han optado por modelos integrales —como los inspirados en el Convenio de Budapest—, México mantiene una estructura reactiva y sectorial, lo que favorece escenarios de impunidad digital estructural.

2. Tipificación penal: insuficiencia normativa y ambigüedad dogmática.

El análisis de la tipificación penal revela que un amplio conjunto de conductas cibernéticas relevantes no cuenta con reconocimiento expreso en el derecho penal mexicano. Fenómenos como el phishing, el ransomware, la usurpación digital de identidad, la manipulación de contenidos mediante deepfakes con fines delictivos o determinadas formas de acoso digital no se encuentran claramente tipificados como delitos autónomos en el CPF.

La ausencia de una tipificación clara y actualizada resulta especialmente problemática en materia de fraude digital, una de las conductas de mayor incidencia en el entorno cibernético mexicano. La doctrina ha señalado que el fraude en línea presenta modalidades específicas —como la publicidad engañosa en internet, la manipulación informativa y el uso de plataformas digitales como medio comisivo— que no encuentran una adecuada correspondencia en los tipos penales tradicionales diseñados para contextos analógicos (Martínez Otero & Miralles Pechuán, 2014).

Esta insuficiencia normativa contrasta con la elevada frecuencia de incidentes relacionados con fraude y usurpación de identidad digital reportados por las autoridades mexicanas, lo que refuerza la necesidad de una reformulación dogmática que atienda las particularidades del entorno digital (INEGI, 2025b; Palazuelos Covarrubias, 2023).

El artículo 211 Bis del CPF, se concentra en conductas básicas de acceso ilícito y alteración de datos, dejando fuera modalidades complejas de ataque a la seguridad informática

y a bienes jurídicos personales y patrimoniales. Esta omisión configura lagunas normativas que dificultan la imputación penal y obligan, en la práctica, a subsumir conductas novedosas en tipos tradicionales diseñados para contextos analógicos, con resultados dogmáticamente insatisfactorios.

Asimismo, el marco penal vigente ofrece respuestas limitadas frente a las formas contemporáneas de autoría y participación en delitos informáticos. La actuación colectiva en entornos digitales, el uso de infraestructuras automatizadas, bots o redes distribuidas de ataque plantea serios desafíos para aplicar las categorías clásicas de autor, coautor o partícipe. A ello se suma la ausencia de una teoría consolidada de imputación objetiva adaptada al ciberespacio, problemática ya advertida por la doctrina mexicana especializada (Alcalá Casillas & Meléndez Ehrenzweig, 2023).

La situación se agrava por la heterogeneidad normativa a nivel estatal. Mientras algunas entidades federativas han incorporado tipos penales relacionados con delitos informáticos, otras carecen de regulación específica, generando un mosaico legislativo desigual. Esta falta de armonización dificulta la determinación de competencias jurisdiccionales y obstaculiza la persecución penal de conductas que, por su propia naturaleza, trascienden fronteras territoriales.

Desde una perspectiva crítica, estos resultados reflejan la dificultad del derecho penal tradicional para adaptarse a un entorno caracterizado por la intangibilidad de las conductas, la anonimidad de los agentes y la ubicuidad del daño. Ello refuerza la necesidad de avanzar hacia una dogmática penal digital, capaz de incorporar estas variables como elementos estructurales del injusto penal.

3. Eficacia institucional y política criminal: impunidad estructural.

Para valorar la eficacia institucional en la persecución de la cibercriminalidad se emplean los indicadores operativos y tipológicos contenidos en el Censo Nacional de

Seguridad Pública Federal y Estatal (CNSPF-E) 2025 del INEGI. Del análisis de las tablas situadas en las páginas 43 a 46 y la tabla de recursos en la página 17, emergen datos que permiten calibrar la respuesta de las autoridades de seguridad pública (INEGI, 2025b).

El censo distingue dos conjuntos de acciones operativas relevantes: ciber patrullajes y ciber investigaciones. En 2024 la Guardia Nacional realizó 4 407 ciber patrullajes y registró 992 ciber investigaciones, en tanto que las policías estatales reportaron 242,943 ciber patrullajes y 15,023 ciber investigaciones (INEGI, 2025b, pp. 43-44). Estas diferencias cuantitativas muestran la mayor intensidad operativa de las policías estatales en tareas de patrullaje preventivo; empero, la sola contabilización de patrullajes no permite inferir eficacia probatoria ni tasa de resolución judicial.

Respecto de los motivos de las ciber investigaciones (Tabla 27, p. 44), el CNSPF-E documenta prioridades distintas entre instancias: para la Guardia Nacional los motivos predominantes fueron “Tráfico de indocumentados” 21.0 % y “Pornografía infantil” 19.7 %, mientras que en las policías estatales prevalecieron “Fraude” 35.5 % y “Amenazas” 13.9 % (INEGI, 2025b, p. 44). Estos contrastes son relevantes desde la política criminal, pues evidencian divergencias en la focalización del riesgo digital y en la asignación operativa de recursos.

En términos de incidencia, el CNSPF-E registra 199,660 incidentes cibernéticos atendidos (Tabla 28, p. 45). La tipología de tales incidentes sitúa en primer lugar el “Robo de contraseñas en redes sociales” 20.1), seguido por “Extorsión” 14.5 y “Acoso” 13.9 %(INEGI, 2025b, p. 45). Estos porcentajes orientan a la dogmática penal sobre los bienes jurídicos más expuestos—identidad digital, patrimonio y autonomía—y permiten priorizar la formación e intervención normativa.

En cuanto a capacidades institucionales, el CNSPF-E indica que 28 instituciones de seguridad pública estatales contaban, al cierre de 2024, con una unidad de policía cibernética

(INEGI, 2025b, p. 17). La existencia de unidades especializadas constituye un avance estructural; no obstante, su sola enumeración exige análisis cualitativos (capacidad del personal, certificación en informática forense, disponibilidad de laboratorios, protocolos de cadena de custodia) para evaluar su real efectividad en la judicialización.

Estos hallazgos confirman la tesis central del estudio: la dispersión normativa y la heterogeneidad operativa —más que la mera ausencia de normas— contribuyen a una respuesta fragmentada frente a la cibercriminalidad. La actividad preventiva (patrullajes) es alta, pero no se traduce necesariamente en efectividad procesal.

Por tanto, la política criminal mexicana requiere no sólo armonización normativa, sino también fortalecimiento técnico-operativo y métricas de resultado (judicialización y sentencias) que permitan evaluar la eficacia real del ius puniendi digital.

La comparación entre las acciones operativas de la Guardia Nacional y las policías estatales, así como la tipología de los incidentes cibernéticos registrados, se resume en la siguiente tabla. Los datos permiten dimensionar la magnitud del trabajo preventivo y la especialización temática de las investigaciones digitales en México.

Tabla 1.

Indicadores operativos y tipología de incidentes.

Indicador / Fuente	**Guardia Nacional**	**Policías Estatales**	**Total / Observación**
Ciber patrullajes (2024)	4 407	242 943	—
Ciber investigaciones (2024)	992	15 023	—
Motivos principales de las ciber investigaciones (Tabla 27) Motivo 1	Tráfico de indocumentados (21.0 %)	Fraude (35.5 %)	—

Motivos principales de las ciber investigaciones (Tabla 27) Motivo 2	Pornografía infantil (19.7 %)	Amenazas (13.9 %)	—
Incidentes cibernéticos atendidos (Tabla 28)	—	—	199 660 (total)
Tipos principales de incidentes (Tabla 28)	—	—	Robo de contraseñas (20.1 %); Extorsión (14.5 %); Acoso (13.9 %)
Unidades de policía cibernética (p. 17)	—	—	28 instituciones estatales

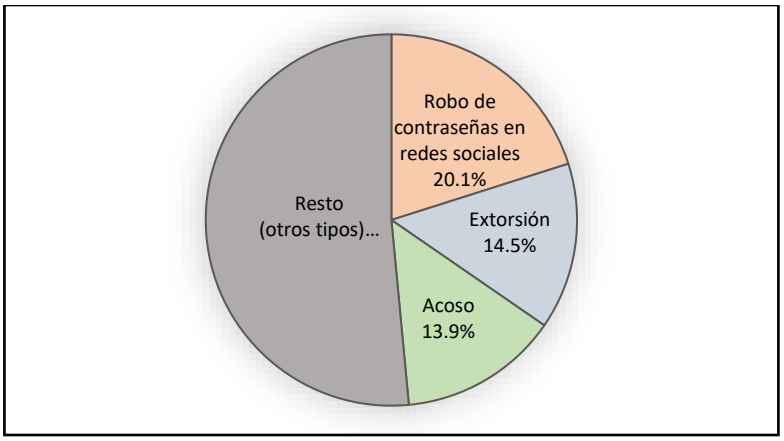
Fuente: Elaboración personal con los datos que aparecen en INEGI (2025), CNSPF-E 2025, pp. 17, 43–46.

Como se aprecia, la mayor carga operativa recae en las policías estatales, y los incidentes de fraude, extorsión y acoso concentran la mayor atención institucional. A continuación, la Figura 2 ilustra la distribución porcentual de los principales tipos de incidentes atendidos en 2024.

Figura 2

Distribución porcentual de tipos de incidentes cibernéticos atendidos (2024).

DOI: https://doi.org/10.71112/d3625c91



Fuente: Elaboración personal con los datos que aparecen en INEGI (2025), CNSPF-E, Tabla 28, p. 45.

A la luz de los datos presentados, la limitada traducción de la actividad operativa en resultados judiciales pone de relieve que la problemática de la cibercriminalidad no se reduce a la detección del delito, sino que involucra el funcionamiento integral del sistema de justicia. La ausencia de protocolos unificados de investigación digital, de estándares comunes de cadena de custodia y de un modelo articulado de justicia digital debilita la capacidad del Estado para procesar eficazmente los delitos informáticos, aun cuando existan unidades especializadas de policía cibernética (INEGI, 2025b). En este sentido, la consolidación de un sistema de justicia digital eficaz se presenta como un elemento indispensable para cerrar la brecha entre investigación y sanción penal (Arley Orduña, 2023).

4. Derecho comparado: lecciones para México.

El análisis comparado muestra que los ordenamientos jurídicos que han avanzado hacia modelos integrales de regulación de la ciberdelincuencia combinan la tipificación penal específica con esquemas de corresponsabilidad de actores privados y mecanismos robustos de protección de datos personales.

En el ámbito europeo, la articulación entre el derecho penal y el Reglamento General de Protección de Datos ha permitido establecer estándares elevados de tutela de derechos

fundamentales, incluyendo obligaciones para plataformas digitales y proveedores de servicios (Reglamento (UE) 2016/679, 2016). Estas tendencias también se reflejan en debates recientes sobre la responsabilidad penal de las plataformas digitales en la prevención de conductas ilícitas, lo que amplía el enfoque tradicional centrado exclusivamente en el autor individual (Campos-Cárdenas & Goyes-Ortiz, 2025).

El análisis comparado revela experiencias legislativas valiosas. En España, la reforma del Código Penal por Ley 1/2015 introdujo modificaciones relevantes en materia de acceso ilícito, interceptación de transmisiones y delitos de sextorsión (Ley Orgánica 1/2015, 2015). Además, el país adoptó plenamente los estándares del Convenio de Budapest, lo que permitió armonizar su normativa penal con los principios de tipicidad y territorialidad internacional.

En Argentina, la Ley 26.388/2008 reformó su Código Penal para incluir la protección de sistemas y datos informáticos, con un enfoque que prioriza la proporcionalidad punitiva y la distinción entre daños patrimoniales y violaciones a la privacidad (Ley 26.388, 2008).

Por su parte, Chile aprobó en junio de 2022 una Ley de Delitos Informáticos (Normas sobre los delitos informáticos, 2022), alineada con el Convenio de Budapest, que incorpora figuras modernas como el fraude informático, la interceptación y la manipulación de datos. Su experiencia demuestra la importancia de un enfoque legislativo unificado y tecnológicamente actualizado.

De estas comparaciones emergen tres lecciones esenciales para México:

1) Unificación normativa: Integrar en un solo cuerpo legal los delitos informáticos dispersos.
2) Definición técnica precisa: Adoptar una terminología informática homogénea, compatible con los estándares internacionales.
3) Cooperación judicial internacional: Ratificar plenamente los mecanismos de cooperación y asistencia mutua previstos por el Convenio de Budapest.

Estas medidas fortalecerían el principio de legalidad y la eficacia en la persecución penal, garantizando al mismo tiempo la protección de derechos fundamentales frente al abuso tecnológico.

Tabla 2.

Comparativo de marcos jurídicos sobre ciberdelincuencia (México, España, Argentina, Chile y Convenio de Budapest).

Jurisdicción	Norma principal	Conductas tipificadas	Enfoque dogmático	Mecanismos de cooperación internacional	Relevancia para México
México	CPF y leyes especiales	Acceso ilícito, daño informático, difusión no consentida	Fragmentado, reactivo	Limitado	Requiere unificación normativa
España	LO 1/2015 y Convenio de Budapest	Acceso, interceptación, sextorsión, fraude	Sistemático, garantista	Pleno	Modelo de armonización legislativa
Argentina	Ley 26.388/2008	Acceso indebido, daño, fraude	Punitivo moderado	Parcial	Claridad técnica en tipificación
Chile	Ley 21.459/2022	Fraude, manipulación, suplantación	Integral	Pleno	Estructura moderna adaptable

UE / Budapest	Convenio 2001	Marco general de tipificación	Supranacional	Pleno y vinculante	Referente técnico y normativo

Fuente: elaboración propia con base a la información recopilada.

Síntesis crítica de los resultados.

Los resultados empíricos y normativos permiten afirmar que la dispersión legislativa que caracteriza al régimen jurídico mexicano en materia de cibercriminalidad constituye un obstáculo estructural para la eficacia del sistema penal. La coexistencia de disposiciones fragmentadas entre el Código Penal Federal, leyes especiales y normativas locales ha dado lugar a un entramado normativo carente de unidad sistemática, que no solo dificulta la interpretación coherente de los tipos penales, sino que debilita de manera significativa la capacidad de persecución y sanción de las conductas delictivas en el entorno digital.

Esta heterogeneidad normativa se traduce, en la práctica, en asimetrías territoriales en la aplicación de la ley, vacíos competenciales y una creciente tendencia hacia la impunidad digital, particularmente visible en delitos de alta incidencia como el fraude electrónico, la usurpación de identidad y diversas modalidades de extorsión.

Desde una perspectiva dogmática, los hallazgos del estudio ponen de relieve la insuficiencia de las categorías penales clásicas para dar cuenta de la complejidad de las conductas desplegadas en el ciberespacio. Conceptos fundamentales como acción, causalidad, autoría, dolo o tentativa, construidos históricamente sobre presupuestos de materialidad y territorialidad, se ven tensionados en escenarios tecnológicos caracterizados por la deslocalización, la automatización y la mediación algorítmica.

La emergencia de formas de coautoría distribuida, de participación indirecta mediante herramientas tecnológicas y de resultados lesivos amplificados en el tiempo y el espacio exige una relectura crítica de los fundamentos del injusto y de la culpabilidad, orientada hacia

modelos de imputación compatibles con la responsabilidad tecnológica, sin sacrificar los principios de legalidad y culpabilidad que informan al derecho penal garantista.

En el plano de la política criminal, los resultados evidencian la necesidad de superar un enfoque predominantemente reactivo, centrado en la respuesta punitiva ex post, para avanzar hacia una estrategia integral, preventiva y prospectiva frente a la cibercriminalidad. Ello implica no solo la actualización normativa, sino también el fortalecimiento de las capacidades institucionales de investigación, la profesionalización técnica de los operadores del sistema de justicia y la incorporación de políticas de alfabetización digital con enfoque judicial.

Ante este escenario, los resultados del análisis permiten sostener que el modelo de regulación vigente resulta insuficiente para ofrecer una respuesta penal coherente frente a la cibercriminalidad. En consecuencia, el debate doctrinal debe orientarse hacia la construcción de un instrumento normativo integral que supere el enfoque fragmentario actual.

En esta línea, la literatura especializada identifica al menos dos alternativas relevantes: por un lado, la elaboración de un Código Penal Digital, que permita sistematizar los tipos penales informáticos dentro de una estructura dogmática unificada; y, por otro, la promulgación de una Ley General de Cibercriminalidad, destinada a establecer principios rectores, definir con precisión las competencias jurisdiccionales, armonizar los tipos penales dispersos y fortalecer los mecanismos de cooperación internacional, indispensables para la persecución eficaz de delitos de naturaleza transnacional.

Asimismo, se vuelve indispensable profundizar en los mecanismos de cooperación internacional para la persecución de delitos transfronterizos, tomando como referencia los estándares establecidos por el Convenio de Budapest y los marcos europeos de ciberseguridad, que ofrecen modelos de coordinación eficaz sin menoscabo de los derechos fundamentales.

El análisis de derecho comparado confirma que es posible construir respuestas penales coherentes, especializadas y respetuosas de las garantías constitucionales frente a la ciberdelincuencia.

Las experiencias de países como España, Argentina o Chile demuestran que la tipificación precisa de los delitos informáticos, acompañada de instrumentos procesales adecuados y de esquemas de cooperación tecnológica, puede fortalecer la eficacia del sistema penal sin derivar en dinámicas de punitivismo excesivo.

Frente a estos referentes, México se encuentra ante una oportunidad histórica para replantear su modelo normativo y avanzar hacia un marco jurídico integral que articule seguridad jurídica, eficacia penal y protección de los derechos humanos en el entorno digital.

En suma, los resultados del estudio no solo ponen en evidencia las limitaciones estructurales del sistema penal mexicano frente a la cibercriminalidad, sino que delinean con claridad las coordenadas de una reforma necesaria: unidad normativa, actualización dogmática, fortalecimiento institucional y cooperación internacional efectiva.

La articulación de estos ejes en una política criminal inteligente y de largo plazo constituye la condición indispensable para transitar de la actual fragmentación hacia un derecho penal digital coherente, funcional y garantista, capaz de responder a los desafíos tecnológicos contemporáneos sin renunciar a los principios fundamentales del Estado constitucional de derecho.

DISCUSIÓN

La discusión de los resultados permite comprender la cibercriminalidad en México no como un problema aislado de tipificación penal, sino como la manifestación de una disfunción estructural del sistema penal frente a la transformación tecnológica.

Los hallazgos confirman que la debilidad de la respuesta estatal no se explica únicamente por la ausencia de ciertos tipos penales, sino por la combinación de fragmentación normativa, insuficiencia dogmática y capacidades institucionales desarticuladas, lo que produce un escenario propicio para la impunidad digital.

En primer lugar, la dispersión normativa identificada no constituye un fenómeno meramente técnico, sino un problema de política criminal. La coexistencia de disposiciones penales en el Código Penal Federal, leyes especiales y códigos estatales, sin criterios dogmáticos comunes ni mecanismos efectivos de coordinación, debilita el principio de legalidad en su dimensión de certeza y previsibilidad.

Lejos de fortalecer la protección de los bienes jurídicos digitales, esta arquitectura fragmentada genera zonas grises de imputación, conflictos competenciales y dificultades probatorias que impactan directamente en la judicialización de los casos.

En este sentido, los resultados empíricos del CNSPF-E 2025 muestran que, aunque existe una actividad operativa considerable, especialmente en materia de patrullaje digital, esta no se traduce necesariamente en investigaciones sólidas ni en resoluciones judiciales efectivas, lo que revela una brecha estructural entre prevención, investigación y sanción.

Desde una perspectiva dogmática, la investigación pone de manifiesto que el derecho penal mexicano continúa operando sobre categorías concebidas para una realidad material y territorial, que resultan insuficientes para explicar la lógica del daño en el ciberespacio. La deslocalización de las conductas, la mediación tecnológica y la posibilidad de resultados lesivos amplificados en el tiempo y el espacio tensionan nociones clásicas como la acción, la causalidad o la autoría.

La ausencia de una teoría consolidada de imputación objetiva en entornos digitales obliga a los operadores jurídicos a forzar la subsunción de conductas complejas en tipos tradicionales, con el consiguiente riesgo de decisiones arbitrarias o de archivo por imposibilidad

técnica de imputación. Esta situación confirma que la discusión sobre la ciberdelincuencia no puede limitarse a la creación de nuevos delitos, sino que exige una reconstrucción teórica de la dogmática penal, compatible con los principios del derecho penal garantista.

En el plano institucional, los datos del INEGI evidencian una respuesta desigual y fragmentada entre los distintos niveles de gobierno. Mientras las policías estatales concentran la mayor parte de los patrullajes y de las investigaciones por fraude, extorsión y acoso digital, la Guardia Nacional prioriza otras tipologías delictivas, lo que refleja la ausencia de una estrategia nacional uniforme de ciberseguridad penal.

La existencia de unidades de policía cibernética en diversas entidades federativas constituye un avance relevante; no obstante, la falta de protocolos unificados de investigación, de estándares comunes de cadena de custodia digital y de indicadores centrados en la judicialización limita de manera significativa su impacto real en la reducción de la impunidad. En este contexto, la impunidad digital aparece menos como una falla individual de los operadores y más como el resultado de un diseño institucional incompleto y descoordinado.

El análisis comparado refuerza estas conclusiones al mostrar que los sistemas jurídicos que han optado por modelos normativos integrales —como España, Argentina o Chile— han logrado una mayor coherencia entre tipificación penal, procedimientos especializados y cooperación internacional. La alineación de estos ordenamientos con los estándares del Convenio de Budapest demuestra que es posible articular una respuesta penal eficaz frente a la ciberdelincuencia sin recurrir a dinámicas de punitivismo excesivo.

Por el contrario, la experiencia mexicana confirma que las reformas parciales y reactivas, aun cuando respondan a demandas sociales legítimas, resultan insuficientes si no se insertan en una visión sistémica de política criminal digital.

A la luz de estos elementos, la discusión permite sostener que el principal desafío para México no radica únicamente en “modernizar” su legislación penal, sino en definir un modelo

coherente de intervención penal en el entorno digital. Ello implica decidir si el sistema continuará respondiendo mediante ajustes fragmentarios o si avanzará hacia un instrumento normativo integral —ya sea un Código Penal Digital o una Ley General de Cibercriminalidad— capaz de armonizar la tipificación, la competencia jurisdiccional y los mecanismos de cooperación nacional e internacional. En cualquiera de los casos, dicha reforma debe partir del principio de última ratio, evitando tanto la inflación penal simbólica como la pasividad normativa que hoy alimenta la impunidad.

En síntesis, la discusión confirma que la cibercriminalidad constituye un problema estructural del derecho penal contemporáneo, que pone a prueba la capacidad del Estado para proteger bienes jurídicos fundamentales en contextos tecnológicos complejos.

México se encuentra ante una coyuntura decisiva: o consolida una política criminal digital coherente, garantista y técnicamente informada, o mantiene un esquema fragmentado que seguirá reproduciendo déficits de seguridad jurídica y desconfianza social.

Los resultados del estudio aportan elementos suficientes para afirmar que la superación de la impunidad digital no depende de respuestas aisladas, sino de una reforma integral que articule dogmática, instituciones y cooperación internacional bajo una lógica común.

CONCLUSIONES

El análisis confirma que el desafío de la cibercriminalidad en México es, en esencia, un problema de arquitectura institucional y adaptación normativa. La dispersión legal, la persistencia de una dogmática anacrónica y la desconexión entre la actividad policial y la eficacia judicial conforman un entramado estructural que favorece la impunidad digital.

Frente a este diagnóstico, las recomendaciones se articulan en una agenda de reforma integral que debe avanzar de manera simultánea en cuatro frentes:

1) Coherencia normativa: La creación de un marco jurídico unificado, mediante una Ley General o un Título Especial, constituye un paso insoslayable para superar la fragmentación legislativa, garantizar la seguridad jurídica y sentar las bases de una persecución penal eficaz.
2) Modernización conceptual: El derecho penal debe incorporar categorías dogmáticas adaptadas a la lógica del ciberespacio, en el que la autoría, la causalidad y la imputación se redefinen a partir de la mediación tecnológica y la deslocalización de las conductas.
3) Efectividad institucional: La reforma normativa debe ir acompañada de herramientas procesales y capacidades técnicas concretas —prueba digital, protocolos especializados y formación continua— que permitan cerrar la brecha existente entre la detección del delito y su judicialización efectiva.
4) Cooperación estructural: Dado el carácter transnacional de la cibercriminalidad, la cooperación nacional e internacional debe dejar de concebirse como un elemento accesorio para consolidarse como un pilar estructural de la política criminal, mediante mecanismos ágiles y alineados con estándares internacionales.

La superación de la impunidad digital no será el resultado de medidas aisladas, sino de una reforma holística y prospectiva. Se trata de construir un ius puniendi digital para México que sea, a la vez, técnicamente eficaz, sistemáticamente coherente y firmemente anclado en las garantías del Estado constitucional de derecho. Este constituye el mandato ineludible para asegurar la vigencia de la justicia penal en el ámbito digital en el siglo XXI.

Declaración de conflicto de interés.

El autor declara no tener ningún conflicto de interés relacionado con esta investigación.

Declaración de contribución a la autoría.

Luis Alfonso Gala Rodríguez: conceptualización, curación de datos, análisis formal, investigación, metodología, administración del proyecto, redacción del borrador original, revisión y edición de la redacción.

Declaración de uso de inteligencia artificial.

El autor declara que hizo uso de inteligencia artificial como apoyo para este artículo, y también que esta herramienta no sustituye de ninguna manera la tarea o proceso intelectual. Después de rigurosas revisiones con diferentes herramientas en la que se comprobó que no existe plagio como constan en las evidencias, el autor manifiesta y reconoce que este trabajo fue producto de un trabajo intelectual propio, que no ha sido escrito ni publicado en ninguna plataforma electrónica o de IA.

REFERENCIAS

Aguirre Quezada, J. P. (2022). *Ciberseguridad, desafío para México y trabajo legislativo* (Cuaderno de investigación). Instituto Belisario Domínguez, Senado de la República. http://bibliodigitalibd.senado.gob.mx/bitstream/handle/123456789/5551/Cuaderno%20de%20Investigaci%C3%B3n%2087.pdf

Alcalá Casillas, M. G. (2024). Desafíos en México sobre la regulación de los ciberdelitos. *Derecom. Revista Internacional de Derecho de la Comunicación y de las Nuevas Tecnologías*, 35, 58–73. https://revistas.ucm.es/index.php/DERE/article/view/98695

Alcalá Casillas, M. G., & Meléndez Ehrenzweig, M. Á. (2023). Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas. *Paakat:*

Revista de Tecnología y Sociedad, 13(24), 1–36. https://doi.org/10.32870/Pk.a13n24.759

Alé Martínez, V. I., & Aguilar Campos, P. (2025). Responsabilidad penal en la era de la inteligencia artificial: De la agencia humana a la autonomía de la *machina sapiens*. *Revista de Estudios de la Justicia*, 42. https://doi.org/10.5354/0718-4735.2025.77061

Arley Orduña, A. M. (2023). Principios para un sistema de justicia digital eficaz en México, a través de la reforma al artículo 17 constitucional. *Boletín Mexicano de Derecho Comparado*. https://doi.org/10.22201/iij.24484873e.2022.164.18092

Cámara de Diputados LXV Legislatura. (2023). *La ciberseguridad: Un estudio comparado*. Centro de Estudios de Derecho e Investigaciones Parlamentarias (CEDIP). https://portalhcd.diputados.gob.mx/PortalWeb/Micrositios/fd7318db-ed1d-4f86-a8f6-1a29b0c49505.pdf

Campos-Cárdenas, F., & Goyes-Ortiz, C. (2025). La responsabilidad penal de las plataformas digitales en la protección de los derechos de propiedad intelectual. *593 Digital Publisher CEIT*, 10(4), 949–960. https://doi.org/10.33386/593dp.2025.4.3407

Cassou Ruiz, J. E. (2009). Delitos informáticos en México. *Revista del Instituto de la Judicatura Federal, Escuela Judicial*, 28, 179–205. https://revistas-colaboracion.juridicas.unam.mx/index.php/judicatura/article/view/32260/29257

Centeno, D. (2018). *México y el Convenio de Budapest: Posibles incompatibilidades*. R3D – Derechos Digitales América Latina. https://www.derechosdigitales.org/wp-content/uploads/minuta_r3d.pdf

Código Penal Federal [CPF]. (2025). *Última reforma publicada el 28 de noviembre de 2025*. Diario Oficial de la Federación. https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf

Consejo de Europa. (2001). *Convenio sobre la ciberdelincuencia* (European Treaty Series No. 185). https://rm.coe.int/1680081561

Consejo de Europa. (2025, 9 de julio). *Adhesión al Convenio sobre la Ciberdelincuencia: Beneficios*. https://rm.coe.int/cyber-buda-benefits-9-julio-2025-es/1680b6b134

Decreto por el que se adicionan diversas disposiciones a la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y al Código Penal Federal (Ley Olimpia). (2021, 1 de junio). *Diario Oficial de la Federación*. https://www.diputados.gob.mx/sedia/biblio/prog_leg/Prog_leg_LXIV/161_DOF_01jun21.pdf

Eslava Zapata, R., Rojas Hermida, C. J., & García Peñaloza, J. E. (2024). Variables asociadas a los delitos informáticos en Latinoamérica. *Academia & Derecho*, 17(28), 1–21. https://dialnet.unirioja.es/descarga/articulo/9637058.pdf

Instituto Nacional de Estadística y Geografía [INEGI]. (2025a). *Censo Nacional de Seguridad Pública Federal 2025: Documento de diseño*. https://www.inegi.org.mx/contenidos/programas/cnspf/2025/doc/889463926108.pdf

Instituto Nacional de Estadística y Geografía [INEGI]. (2025b). *Censo Nacional de Seguridad Pública Federal y Estatal 2025: Resultados*. https://www.inegi.org.mx/contenidos/programas/cnspe/2025/doc/cnspe_2025_resultados.pdf

Ley 26.388. (2008). *Delitos informáticos*. República Argentina. https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto

Ley Federal de Protección de Datos Personales en Posesión de los Particulares [LFPDPPP]. (2010). *Diario Oficial de la Federación*. https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Ley Orgánica 1/2015. (2015). *Reforma del Código Penal*. Boletín Oficial del Estado. https://www.boe.es/eli/es/lo/2015/03/30/1/con

Maculan, E., Anckar, H., Malarino, E., & Gil Gil, A. (Eds.). (2024). *Nuevas tecnologías y sistema penal: Un estudio de los ordenamientos latinoamericanos*. Konrad-Adenauer-Stiftung e. V. https://www.kas.de/documents/271408/16552318/Nuevas+tecnolog%C3%ADas+y+sistema+penal.pdf

Martínez Otero, J. M., & Miralles Pechuán, L. (2014). Fraudes en la publicidad en internet: Tipología y tratamiento jurídico. *Revista Aranzadi de Derecho y Nuevas Tecnologías*, 34, 67–90. https://dialnet.unirioja.es/servlet/articulo?codigo=4670295

Naciones Unidas. (2025). *Convención de las Naciones Unidas contra la Ciberdelincuencia*. Oficina de las Naciones Unidas contra la Droga y el Delito. https://www.unodc.org/unodc/es/cybercrime/convention/text/convention-full-text.html

Normas sobre los delitos informáticos, Ley 21.459. (2022). Biblioteca del Congreso Nacional de Chile. https://www.bcn.cl/leychile/navegar?idNorma=1177743

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

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo. (2016). *Reglamento General de Protección de Datos*. Diario Oficial de la Unión Europea. https://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=uriserv:OJ.L_.2016.119.01.0001.01.SPA

Segundo Protocolo Adicional al Convenio sobre la Ciberdelincuencia, relativo a la cooperación reforzada y la revelación de pruebas electrónicas. (2023). *Diario Oficial de la Unión Europea*, L 63, 28–63. https://eur-lex.europa.eu/legal-content/ES/AUTO/?uri=uriserv:OJ.L_.2023.063.01.0028.01.SPA