ppi 201502ZU4645
Esta publicación científica en formato digital es continuidad de la revista impresa
ISSN-Versión Impresa 0798-1406 / ISSN-Versión on line 2542-3185Depósito legal pp
197402ZU34

CUESTIONES POLÍTICAS

Instituto de Estudios Políticos y Derecho Público "Dr. Humberto J. La Roche"
de la Facultad de Ciencias Jurídicas y Políticas de la Universidad del Zulia
Maracaibo, Venezuela

Vol.43 Nº 83
Julio
Diciembre
2025

Cuestiones Políticas Vol. 43, Nº 83 (2025), 42-55
IEPDP-Facultad de Ciencias Jurídicas y Políticas - LUZ

Responsabilidad penal por manipulación digital con fines delictivos: Una mirada desde el derecho digital comparado en América Latina

Paola Margoth Sánchez Salazar *
Ayrton Andrés Araujo Arízaga **
Fabián Marcelo Salinas Herrera ***

Resumen

En la realidad actual, caracterizada por la hegemonía de lo tecnológico en todos los ámbitos de la vida social, discutir sobre la responsabilidad penal por la manipulación digital con intenciones delictivas en América Latina implica abordar un ámbito teórico y práctico complicado, que supera en muchos aspectos las antiguas líneas del delito convencional para adentrarse en el rápido desarrollo del ciberespacio, dentro de la estructura constante de la sociedad digital del siglo XXI. Por estas razones, el objetivo de la investigación fue analizar el alcance y significado doctrinal de la responsabilidad penal por manipulación digital con fines delictivos, desde la óptica del derecho digital comparado latinoamericano. Para el logro de este objetivo, se hizo uso de la hermenéutica jurídica, en el marco de la metodología del derecho comparado. Los resultados obtenidos permiten concluir que, no hay una única respuesta contundente a la pregunta ¿hasta qué punto es posible atribuir responsabilidad penal cuando el agente del delito se oculta tras algoritmos y redes dispersas? más bien, la doctrina va construyendo, tropezando, reinventando las bases de la imputación y del bien jurídico en juego, a medida que los casos reales desafían los marcos jurídicos que se creían seguros.

Palabras clave: responsabilidad penal; manipulación digital; derecho comparado; América Latina; derecho digital.

* Abogada e Ingeniera Empresarial con Máster en Derecho Penal. Universidad Católica de Cuenca, extensión la troncal. ORCID ID: https://orcid.org/0000-0002-3024-2962. Email: paola.sanchez@ucacue.edu.ec

** Estudiante de la Universidad Católica de Cuenca, extensión la Troncal. ORCID ID: https://orcid.org/0009-0009-4292-0757. Email: ayrton.araujo@est.ucacue.edu.ec

*** Abogado con un Magister en derecho constitucional, mención Procesal Constitucional. Universidad Católica de Cuenca. ORCID ID: https://orcid.org/0000-0001-6468-1878. Email: fsalinash@ucacue.edu.ec

Recibido el 19/06/25 Aceptado el 12/08/25

Criminal liability for digital manipulation for criminal purposes: A look at comparative digital law in Latin America

Abstract

In today's world, characterized by the hegemony of technology in all areas of social life, discussing criminal liability for digital manipulation with criminal intent in Latin America involves addressing a complex theoretical and practical field that in many ways goes beyond the old lines of conventional crime and delves into the rapid development of cyberspace within the constant structure of the digital society of the 21st century. For these reasons, the objective of the research was to analyze the scope and doctrinal significance of criminal liability for digital manipulation with criminal intent from the perspective of comparative Latin American digital law. To achieve this objective, legal hermeneutics was used within the framework of comparative law methodology. The results obtained allow us to conclude that there is no single definitive answer to the question: to what extent is it possible to attribute criminal responsibility when the perpetrator of the crime hides behind algorithms and dispersed networks? Rather, doctrine is constructing, stumbling, and reinventing the bases of imputation and the legal right at stake, as real cases challenge legal frameworks that were believed to be secure.

Keywords: criminal liability; digital manipulation; comparative law; Latin America; digital law.

Introducción

Hablar de la responsabilidad penal por manipulación digital con fines delictivos en América Latina es entrar en terreno complejo, dejando de lado las viejas fronteras del delito tradicional para adentrarse en el acelerado avance del ciberespacio en la configuración permanente de la sociedad digital del siglo XXI. Según indica Pérez (2021), el derecho penal se enfrenta hoy a una metamorfosis obligada: debe adaptarse a la desterritorialización y el anonimato propios de la cibercriminalidad, como bien lo muestra la problemática latinoamericana y mundial, donde los sistemas judiciales luchan por no quedar rezagados frente a las sofisticadas técnicas digitales empleadas para delinquir. A veces, todos hemos sentido que, en el mundo de hoy, la ley va intentándolo, pero, entre avances tecnológicos y vacíos legislativos, la persecución penal queda en la cuerda floja.

En este hilo conductor, el reconocimiento jurídico de la manipulación digital como un tipo delictivo particular, presenta un reto que trasciende

la interpretación convencional del dolo y la culpa. Por lo tanto, conviene preguntar entonces ¿Cómo penalizar de manera adecuada conductas en las que la responsabilidad puede ser ambigua y el perjuicio virtual supera las fronteras nacionales? En América Latina, el análisis jurídico, tal como suponen Eslava-Zapata *et al*., (2024), muestra una tendencia, más allá de toda duda razonable, hacia el aumento de normativas específicas que incluyen delitos cibernéticos y establecen nuevas categorías relacionadas con el mal uso de las tecnologías. No obstante, desde nuestro punto de vista, lo que a menudo escasea es una articulación doctrinal sólida, que pueda abordar los dilemas del derecho digital en un ecosistema legal y tecnológico en continua transformación.

Antes estas preocupaciones legales, el objetivo central de esta investigación es analizar el alcance y significado doctrinal de la responsabilidad penal por manipulación digital con fines delictivos, desde la óptica del derecho digital comparado latinoamericano. De este objetivo surgen tres inquietudes filosófico-jurídicas que nos guiaron a lo largo de esta investigación: ¿Hasta qué punto es posible atribuir responsabilidad penal cuando el agente del delito se oculta tras algoritmos y redes dispersas? ¿Qué límites éticos debería imponerse en el derecho penal ante la manipulación digital? Y no menos importante ¿Hasta dónde debe reformarse el marco normativo para proteger bienes jurídicos ante amenazas emergentes que rebasan la lógica tradicional del delito?

Sin ninguna duda, el derecho digital comparado latinoamericano constituye un método muy útil para identificar similitudes, divergencias y vacíos normativos. De hecho, en palabras de Fernandes y Díaz (2022), aplicar el derecho comparado como herramienta investigativa permite contrastar la efectividad de modelos regulatorios y doctrinales de varios países diferentes —lo cuales, más allá de sus particularidades— enfrentando problemas estructurales comunes a toda la región. De modo que, lejos de ser un ejercicio académico exótico, el análisis comparado ayuda a cuestionar supuestos y promover el intercambio de buenas prácticas, así como propiciar reformas legislativas más acordes con la realidad digital latinoamericana.

En lo concreto, esta investigación se organiza en cuatro secciones generales para entender el fenómeno de estudio en toda su complejidad sustancial: en la primera, se presenta el marco teórico, profundizando en los conceptos clave y el estado del arte; en la segunda sección, se explica la metodología utilizada, con énfasis en el enfoque comparativo y los métodos de estudio interdisciplinarios; en la tercera, se lleva a cabo un análisis crítico y la consiguiente discusión de resultados. Por su parte, la cuarta y última sección, ofrece las conclusiones del estudio, donde además se exponen las propuestas y desafíos pendientes para un derecho penal realmente adaptado a la era digital del siglo XXI.

1. Bases teóricas

En líneas genérales, la responsabilidad penal por manipulación digital con fines delictivos implica la atribución jurídica de consecuencias penales a quienes utilizan herramientas digitales para cometer delitos, ya sea modificando, alterando, o eliminando información con el propósito de obtener un beneficio ilícito o causar daño a terceros. Por ejemplo, el fraude informático mediante la manipulación de datos bancarios para transferir dinero sin consentimiento encarna, claramente, esta clase de responsabilidad penal. Se trata de conductas dolosas o imprudentes que, aunque se desarrollan en espacios virtuales, afectan bienes jurídicos fundamentales reconocidos por el derecho penal contemporáneo. En palabras de Mayer y Oliver:

> Más aún, el estudio sistemático del cibercrimen surge, precisamente, debido a la comisión de fraudes informáticos asociados a transferencias electrónicas de fondos, hace aproximadamente tres décadas... Hasta la fecha, el fraude informático ha continuado siendo el centro de los ciberdelitos, básicamente por el impacto económico y la frecuencia práctica que caracteriza a su ejecución, la que a su turno se ha visto potenciada por el auge del comercio electrónico. (2020, p. 152)

En el estado actual del debate sobre derecho digital, las posturas doctrinales oscilan entre quienes consideran que los delitos informáticos deben ser regulados bajo las mismas reglas del derecho penal tradicional y; quienes, por su parte, proponen la construcción de nuevos modelos jurídicos que respondan a la naturaleza descentralizada y transnacional de estos delitos. Algunos juristas, como es el caso de quienes desarrollaron esta investigación, insisten en que la manipulación digital, al difuminar la autoría y aprovechar el anonimato del entorno virtual, exige una revisión profunda de los modelos de imputación y prueba, como apunta la legislación española en el caso de las estafas informáticas (Devia, 2017).

En Palabras de Mayer (2017), un enfoque alternativo en el debate sugiere que los delitos informáticos requieren una protección independiente en relación con los bienes jurídicos perjudicados, como el sistema de información y la integridad digital, sin limitarse a las categorías tradicionales de patrimonio, intimidad o libertad. En ocasiones, al examinar los ciberataques, la dificultad técnica provoca que jueces y fiscales requieran nuevos criterios de prueba y de interpretación. En el ámbito latinoamericano, resalta la inquietud por la regulación inadecuada y la carencia de actualización normativa ante el rápido progreso de la tecnología. En este orden de ideas, queda claro que:

> El bien jurídico cumple funciones de gran relevancia para las ciencias penales. Entre ellas, la afectación de un bien jurídico permite fundamentar el castigo punitivo de las conductas que lo lesionan o popenalnen en peligro y constituye un requisito ineludible para el ejercicio del ius puniendi. (Mayer, 2017, p. 235)

Un artículo imprescindible para entender el marco conceptual de los delitos digitales es el trabajo de Mayer y Oliver (2020), en el que se estudia cómo la manipulación digital constituye una acción típica que lesiona la confianza y la seguridad en los sistemas informáticos. Los autores exponen la evolución doctrinal que ha llevado a incluir conductas como el phishing, las estafas a través de software malicioso y las transferencias ilícitas de fondos, mostrando la progresiva sofisticación del fraude digital y el reto permanente para los sistemas jurídicos. Por su parte, la investigación "El tratamiento penal de los delitos cometidos a través de Internet" de la autoría de Devia (2017), profundiza en cómo los cambios legislativos han intentado responder a la demanda social de protección frente a formas inéditas de fraude y manipulación digital. El texto muestra que, al menos en España, el legislador ha creado tipos penales diferenciados, incluyendo actos preparatorios como la fabricación de software destinado a la comisión de delitos y, además, destaca las controversias doctrinales respecto a la atribución de responsabilidad penal y la interpretación de las nuevas figuras legales.

En una mirada de síntesis doctrinal, la evolución del concepto de responsabilidad penal por manipulación digital con fines delictivos refleja una paradoja filosófica y práctica entre la salvaguarda de bienes jurídicos emergentes y la imperiosa necesidad de ajustar la dogmática penal a contextos virtuales impredecibles. En efecto, tanto la normativa como la interpretación judicial son, hasta cierto punto, "proyectos en desarrollo", influenciados por controversias constitucionales, éticas y tecnológicas de difícil resolución. Todo esto nos presenta, sin duda, un terreno propicio para continuar reflexionando y transformando el derecho penal –en ocasiones hallando que las respuestas más adecuadas no residen en los códigos, sino en la imaginación y el sentido crítico de quienes los ejecutan, investigan y reflexionan sobre estos asuntos.

2. Metodología

El presente estudio actual emplea un diseño metodológico de tipo documental, basado en la hermenéutica jurídica como fundamento para la interpretación y el análisis crítico de los textos legales y doctrinales identificados. Esta metodología facilita no solo la comprensión de los contenidos normativos, sino también la creación de nuevas visiones mediante el intercambio con el contexto sociopolítico y tecnológico de los crímenes digitales. De este modo, la hermenéutica jurídica, al decir de Botero (2015), adquiere una relevancia inusitada, al permitir interpretaciones profundas, en la reconstrucción legal de casos de manipulación y fraude digital, como lo muestran investigaciones recientes sobre metodologías legales aplicadas en esta área de investigación emergente.

Cuadro 1. Mapa conceptual de la arquitectura metodológica comparativa.

Fuente: elaborado por los autores (2025).

Aunado a lo anterior, se empleó también la metodología del derecho comparado, herramienta esencial cuando se busca identificar similitudes y diferencias de las respuestas normativas frente a la responsabilidad penal por manipulación digital, en países como: Perú, México, Colombia, Venezuela y Ecuador. Tal como afirma Somma (2015), el análisis radicalmente comparativo, mucho más allá de ser un trámite formal, permite descubrir los matices, silencios y contradicciones de cada sistema jurídico respecto al procesamiento penal de la evidencia digital, en los cinco países focalizados. Esta estrategia indagatoria ayuda a comprender cómo evoluciona la realidad normativa en la región y cuáles son los puntos de convergencia o fricción más evidentes. Por lo demás:

> Los comparatistas suelen introducir su materia definiéndola como una reacción al estudio de los derechos nacionales, cuyos autores se reputan de poco preparados para valorar puntos de vista alternativos a los típicos del ordenamiento del que proceden. Por el contrario, la atención a derechos diferentes al propio lleva al comparatista a asumir una pluralidad de puntos de vista, a cuestionar por tanto certezas adquiridas, a poner en duda lo que otros consideran verdades indiscutibles. (Somma, 2015, p. 19)

La investigación se desarrolló en cuatro etapas bien definidas. Primero, se efectuó la búsqueda y revisión exhaustiva de literatura científica, normativa y jurisprudencial sobre manipulación digital y responsabilidad penal. La

segunda etapa consistió en el análisis conceptual y la sistematización de las normas latinoamericanas relevantes. En un tercer momento, se realizó el contraste comparativo normativo y doctrinal, tanto intra como entre los países objeto de estudio. Por último, la síntesis de hallazgos y la construcción de conclusiones propiciaron la consolidación teórica y práctica del estudio, dejando abiertas nuevas rutas de investigación de un tema fértil que esta, en constante desarrollo.

3. Análisis y discusión de los resultados

La normativa ecuatoriana en materia de responsabilidad penal por alteraciones digitales con fines delictivos muestra notables carencias tanto en la definición como en la penalización de estas acciones. El Código Orgánico Integral Penal (COIP) establece normas sobre fraudes en línea, acceso no autorizado y suplantación de identidad (Asamblea Nacional de la República de Ecuador, 2014), pero también posee importantes lagunas, sobre todo ante el progreso tecnológico y la complejidad de los delitos cibernéticos. Por ejemplo, el artículo 190 penaliza la manipulación informática relacionada con apropiaciones fraudulentas, pero la vaguedad y extensión de la norma complican la persecución y castigo efectivos de los culpables, además de crear inseguridad jurídica para las víctimas.

> Art. 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años. La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes. (Asamblea Nacional de la República de Ecuador, 2014)

En palabas de Sarmiento-Chamba y Maldonado-Ruiz (2024), otro aspecto crítico en Ecuador es la insuficiencia de penas y la falta de sanciones económicas adecuadas. Analizando el uso indebido de sistemas informáticos y la distribución de software malicioso, los autores señalan la urgencia de reformar el COIP y adherirse al Convenio de Budapest para mejorar la cooperación internacional y adaptarse a los escenarios globalizados que identifican al mundo actual. Para quienes suscriben esta investigación, el ciberacoso y la suplantación de identidad también son problemáticas crecientes, mostrando que la legislación ecuatoriana sigue siendo estrictamente reactiva, sin contemplar estrategias preventivas ni,

mucho menos, políticas de educación digital que fortalezcan la protección de los derechos de la ciudadanía.

Por su parte, en Perú, la Ley 30096 y sus enmiendas (Presidente de la República del Perú, 2014) castiga el fraude cibernético, la usurpación de identidad y el mal uso de los dispositivos digitales, imponiendo penas de hasta nueve años para acciones agravadas o reincidentes. No obstante, su implementación práctica muestra desafíos significativos, tales como: los fiscales comunes, sin formación especializada, han recibido históricamente denuncias de ciberdelitos, complicando la investigación y el enjuiciamiento, lo que ha dado lugar a altas tasas de impunidad y un lento aprendizaje institucional, según afirma Alcantara (2024). La ratificación del Convenio de Budapest ha reforzado la capacidad de persecución penal y la cooperación internacional, pero la evolución tecnológica constante requiere una actualización casi continua del marco legal.

En el contexto peruano, el delito de suplantación digital es especialmente relevante, pues la ley diferencia la gravedad según la edad de la víctima y el perjuicio causado. Asimismo, se han desarrollado disposiciones específicas para el chantaje sexual mediado por tecnología y el abuso de mecanismos informáticos. La ley reconoce el daño moral y patrimonial como agravante, y exige la especialización de los operadores penales. En este orden de ideas, todo indica que el reto radica en el ritmo acelerado de la ciberdelincuencia, que obliga al Estado y la sociedad a mantener esquemas flexibles de reacción frente a las nuevas modalidades de manipulación, por lo demás el objeto de la ley a la prevención y sanción del ciberdelito en todas sus manifestaciones:

> La presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia. (Presidente de la República del Peru, 2014: art. 1)

En Venezuela, la Ley Especial Contra Delitos Informáticos (2001) (La Asamblea Nacional de la República Bolivariana de Venezuela, 2001) y la Ley de Infogobierno (La Asamblea Nacional de la República Bolivariana de Venezuela, 2013) regulan una variedad de delitos relacionados con el uso indebido de las tecnologías de la información. La manipulación de datos, la oferta engañosa y la falsificación de documentos electrónicos son objeto de tipificación y sanción, existiendo agravantes según el daño económico o patrimonial. Una crítica relevante a estas y otras leyes similares, es la falta de actualización permanente y la limitada digitalización judicial, que ralentiza la investigación y la respuesta estatal ante delitos muy específicos, como la venta fraudulenta por redes sociales. Por lo demás, la ley de 2001 tiene como propósito la protección integral de personas y sistemas informáticos:

> Artículo 1. Objeto de la Ley. La presente Ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la

> prevención y sanción de los delitos cometidos contra tales sistemas o cualesquiera de sus componentes, o de los delitos cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta Ley. (La Asamblea Nacional de la República Bolivariana de Venezuela, 2001)

Queda claro que, en Venezuela la legislación que regula esta materia se centra en la protección integral de sistemas informáticos y bienes jurídicos digitales por igual, incluyendo la privacidad y los datos de sus ciudadanos. El legislador diferencia entre falsificación de firmas electrónicas, sabotaje informático y fraudes financieros, dotando a la Ley de un abanico de medidas preventivas y punitivas. Sin embargo, en la actualidad queda pendiente un mayor control sobre el uso de inteligencia artificial en los procesos judiciales, así como la inclusión de delitos emergentes a la luz de nuevas tecnologías y plataformas digitales.

Como sucede en los casos anteriores, en Colombia, la responsabilidad penal por manipulación digital se sustenta en el Código Penal (El Congreso de Colombia, 2000) y la Ley 1273 de 2009 (El Congreso de Colombia, 2009), que tipifican la interceptación ilegal de datos, el daño informático y el robo de información digital. En estos cuerpos normativos, se contemplan penas de hasta ocho años y sanciones económicas, diferenciando entre delitos agravados y modalidades atenuadas. No obstante, la doctrina señala la existencia de brechas legales y la necesidad de un equilibrio constante entre la protección de la privacidad y el avance de la tecnología.

Tal como sostiene Alvarado (2017), lo más interesante en el caso colombiano es la atención prestada a la protección del derecho a la intimidad y la importancia de la especialización judicial en temas de ciberseguridad. De esta manera, el sistema penal se apoya en medidas cautelares para la protección y restauración de los derechos de las víctimas, pero la velocidad de las transformaciones tecnológicas sigue superando la capacidad de adaptación legislativa. Es común, sin embargo, hallar dificultades probatorias y en la interpretación judicial de pruebas.

México, a su vez, ha progresado en la integración de delitos nuevos vinculados a la manipulación digital, como la tipificación de la violencia digital, el uso indebido de sistemas de inteligencia artificial y la generación de *deepfakes*. Las modificaciones al Código Penal Federal (Cámara de Diputados del H. Congreso de la Unión, 2025), tienen como objetivo fijar sanciones adecuadas y distinguir entre conductas severas y menores, aunque el debate sobre la idoneidad de la tipificación continúa. La salvaguarda de derechos fundamentales, especialmente en cuestiones de privacidad y reputación, representa uno de los aspectos más sensibles y debatidos en la legislación mexicana.

Por estas razones, Morán (2020) afirma que, la legislación mexicana revela una preocupación creciente por los impactos de la inteligencia artificial

y las tecnologías avanzadas sobre la criminalidad digital. Aunque se han promulgado iniciativas para fortalecer la sanción de delitos informáticos, aún persisten retos ligados a la efectiva protección de los grupos más vulnerables del entorno digital y la actualización constante de las normas ante el desarrollo de nuevas herramientas digitales con potencial delictivo.

Cuadro 2. Visión comparativa de la justicia sobre delitos digitales.

País	Norma Principal	Conductas Tipificadas	Penas	Desafíos/Limitaciones
Ecuador	COIP (Art. 190, 211, 234, 166).	Fraudes, acceso ilícito, suplantación, ciberacoso.	1-3 años de prisión; penas que en muchos casos configuran sanciones insuficientes o ambiguas.	Reformas urgentes, vacíos normativos, cooperación internacional.
Perú	Ley 30096, DL 1591, Código Penal.	Fraude informático, suplantación, abuso de dispositivos tecnológicos.	1-9 años de prisión y multas.	Actualización constante, especialización fiscal, adherencia Budapest.
Venezuela	Ley Especial Contra Delitos Informáticos, Ley Infogobierno.	Oferta engañosa, falsificación documentos, fraude y suplantación de identidad.	3-6 años de prisión y multas; agravantes.	Protección integral, sanciones diferenciadas y digitalización judicial.
Colombia	Cód. Penal, Ley 1273/2009, Ley 1581/2012.	Interceptación de datos, daño informático, robo y sabotaje digital.	3-8 años de prisión y multas.	Brechas legales, protección privacidad, adaptación constante a las nuevas tecnologías.
México	Código Penal Federal (reformas nuevas).	Violencia digital, suplantación, deepfakes, fraude, IA.	Sanciones proporcionales, aún en revisión.	Tipificación insuficiente, retos IA, derechos fundamentales.

Fuente: elaborado por los autores (2025), con base a las leyes consultadas.

El cuadro comparativo 2 resume las tendencias y retos más importantes en responsabilidad penal por manipulación digital en los cinco países estudiados. Se nota que, a pesar de que todos los países abordados cuentan con marcos legales concretos, las sanciones y clasificaciones difieren dependiendo de la gravedad y el impacto del daño, y cada nación enfrenta desafíos particulares en la modernización de sus legislaciones, la especialización de los operadores judiciales y la protección real de los derechos digitales. En términos generales, las reformas y el fortalecimiento de la colaboración internacional son asuntos clave en América Latina, junto con la capacitación técnica y legal continua. Y es que, definitivamente, todo sistema legal presenta progresos, incertidumbres e imperfecciones inherentes, pero todos se unen en la búsqueda de respuestas al fenómeno creciente y diverso de la manipulación digital delictiva.

Conclusiones

Nuestra experiencia en el área objeto de estudio sugiere que, mirando en retrospectiva, definir el alcance y significado doctrinal de la responsabilidad penal por manipulación digital en Latinoamérica, desde lo digital comparado, es como intentar atrapar humo con las manos. Siempre parece que, cuando se cree tener una fórmula jurídica clara, la realidad cambia de forma otra vez. El derecho, tradicionalmente rígido, está obligado a bailar al ritmo frenético de la tecnología, y —honestamente— a veces parece que esto es imposible de lograr. Por lo tanto, no hay una única respuesta contundente a la pregunta ¿hasta qué punto es posible atribuir responsabilidad penal cuando el agente del delito se oculta tras algoritmos y redes dispersas? más bien, la doctrina va construyendo, tropezando, reinventando las bases de la imputación y del bien jurídico en juego, a medida que los casos reales desafían los marcos que creíamos seguros.

Ahora, cuando pensamos en cómo atribuir responsabilidad penal a quien se oculta tras las líneas de código, viene la sensación de que estamos corriendo detrás de las sombras. ¿Cómo culpar, con rigor, a un "autor" difuso en una telaraña de algoritmos y servidores remotos? Por momentos esta situación resulta francamente frustrante. Aun así, el desafío invita a ajustar la lupa de la investigación científica, mezclar el derecho con la pericia técnica, y buscar caminos inéditos. Y es que ¿Quién dijo que el proceso penal no podía aprender de los hackers éticos? Es un campo por descubrir, y —quien lo niegue— no está viendo el tamaño del problema.

¿Qué límites éticos debería imponerse en el derecho penal ante la manipulación digital?

> En el plano ético, cuesta mucho no tentarse con el *punitivismo* a ultranza. A veces, leyendo hermenéuticamente propuestas legislativas, parece que el miedo guía más que el sentido común. Vale la pena recordarnos que el derecho penal, también en lo digital, debe cuidar la dignidad y las garantías básicas de la persona humana, por lo tanto, no podemos apresurarnos a castigar sin medir las consecuencias. La ética, reside más en esa mesura, algo casi artesanal en estos tiempos de inmediatez, que en la mera inclusión de términos grandilocuentes en la ley. en este hilo conductor, un poco de autocrítica nunca sobra: la inteligencia artificial no puede justificar la inteligencia punitiva desmedida.

Pero entonces ¿Hasta dónde debe reformarse el marco normativo para proteger bienes jurídicos ante amenazas emergentes que rebasan la lógica tradicional del delito? Para responder a esta legítima interrogante conviene interpelar, en principio, sobre el sentido de reformar sin pausa los marcos legales para protegernos de amenazas imprevistas. La tentación de legislar desde el miedo al cibercrimen parece riesgosa. No negamos que hacen falta reformas profundas en Latinoamérica; las cuales llenaran en su momento los vacíos de las leyes actuales. Pero reformar sin el debido razonamiento

y con base a la evidencia empírica concreta de cada país, puede ser igual de peligroso que dejar todo como está. A veces pasa que, mientras más sabemos, más preguntas surgen —y es, precisamente, en esas preguntas donde se encuentra el verdadero potencial transformador del derecho.

Por último, debemos aclarar que esta investigación tiene sus límites y, quizás, más de los que uno quisiera admitir. La mirada documental y el derecho comparado ayudan, pero dejan espacios grises y rincones problemáticos sin explorar. Hay veces que quisimos acceder a datos o testimonios reales y simplemente no estaban ahí, y otros momentos donde se limitó la precisión del dato por profundidad teórica. No vemos esto como fracaso, más bien supone un recordatorio sincero de lo humano en el propio trabajo académico. Y es que estamos siempre en proceso, aprendiendo, corrigiendo, y —en nuestro caso— todavía dudando si el último párrafo podría haber sido mejor, dicho de otra forma, para desarrollar futuras investigaciones sobre el tema con mayor precisión teórica y conceptual.

Referencias Bibliográficas

ALCANTARA, Fabian. 2024. “Análisis de la ley 30096 de delitos informáticos en su aplicación a los delitos de fraude informático en el Perú, 2022” En: Universidad Señor de Sipán. Disponible en línea. En: https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/12384/Alcantara%20Diaz,%20Fabian%20Eduardo.pdf. Fecha de consulta: 14 de marzo de 2024.

ALVARADO, Manuel. 2017. “Aspectos legales al utilizar las principales redes sociales en Colombia” En: Revista Logos, Ciencia & Tecnología. Vol. 8, No. 2, pp. 211-220. Disponible en línea. En: https://doi.org/https://www.redalyc.org/journal/5177/517752177019/html. Fecha de consulta: 14 de marzo de 2024.

ASAMBLEA NACIONAL DE LA REPUBLICA DE ECUADOR. 2014. Código Orgánico Integral Penal, COIP. Disponible en línea. En: https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/03/COIP_act_feb-2021.pdf. Fecha de consulta: 10 de febrero de 2025.

BOTERO, Andrés. 2015. “La metodología documental en la investigación jurídica: alcances y perspectivas” En: Revista Opinión Jurídica. Vol. 2, No. 4, pp. 109-116. Disponible en línea. En: https://revistas.udem.edu.co/index.php/opinion/article/view/1350/1373. Fecha de consulta: 18 de abril de 2025.

CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN. 2025. Código Penal Federal. Disponible en línea. En: https://www.diputados.gob.mx/LeyesBiblio/pdf/CPF.pdf. Fecha de consulta: 7 de julio de 2024.

DEVIA, Edmundo. 2017. "Delito Informático: Estafa Informática del Artículo 248.2 del Código Penal" En: Universidad de Sevilla. Disponible en línea. En: https://idus.us.es/server/api/core/bitstreams/885069f5-7725-4bd9-858f-3320feb75da1/content. Fecha de consulta: 18 de abril de 2025.

EL CONGRESO DE COLOMBIA. 2000. Ley 599 de 2000 por la cual se expide el Código Penal. Disponible en línea. En: https://www.oas.org/dil/esp/codigo_penal_colombia.pdf. Fecha de consulta: 24 de julio de 2024.

EL CONGRESO DE COLOMBIA. 2009. LEY 1273 DE 2009. Disponible en línea. En: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492. Fecha de consulta: 5 de enero de 2025.

ESLAVA-ZAPATA, Rolando; ROJAS-HERMIDA, Carlos; GARCÍA-PEÑALOZA, John. 2024. "Variables asociadas a los delitos informáticos en Latinoamérica" En: Revista Academia & Derecho. Vol. 15, No. 28, pp. 1-21. Disponible en línea. En: https://doi.org/https://doi.org/10.18041/2215-8944/academia.28.11822. Fecha de consulta: 5 de enero de 2025.

FERNÁNDEZ, Eder; DÍAZ, José. 2022. Los derechos digitales: ¿hacia una nueva generación de derechos humanos? Aproximaciones teóricas desde América Latina y Europa" En: Direito, Estado e Sociedad. No. 61, pp. 80-105. Disponible en línea. En: https://revistades.jur.puc-rio.br/index.php/revistades/article/view/1942/727. Fecha de consulta: 15 de marzo de 2025.

LA ASAMBLEA NACIONAL DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA. 2001. Ley Especial Contra los Delitos Informáticos. Disponible en línea. En: https://www.oas.org/juridico/spanish/mesicic3_ven_anexo18.pdf. Fecha de consulta: 15 de marzo de 2025.

LA ASAMBLEA NACIONAL DE LA REPÚBLICA BOLIVARIANA DE VENEZUELA. 2013. Ley de Infogobierno. Disponible en línea. En: http://www.ucv.ve/fileadmin/user_upload/facultad_farmacia/Documentos/leyinfog.pdf. Fecha de consulta: 10 de octubre de 2024.

MAYER, Laura. 2017. "El bien jurídico protegido en los delitos informáticos" En: Revista Chilena de Derecho. Vol. 44, No. 1, pp. 235-260. Disponible en línea. En: https://www.scielo.cl/pdf/rchilder/v44n1/art11.pdf. Fecha de consulta: 10 de octubre de 2024.

MAYER, Laura; OLIVER, Guillermo. 2020. "El delito de fraude informático: Concepto y delimitación" En: Revista chilena de derecho y tecnología. Vol. 9, No. 1, pp. 151-184. Disponible en línea. En: https://www.scielo.cl/

pdf/rchdt/v9n1/0719-2584-rchdt-9-1-00151.pdf. Fecha de consulta: 25 de enero de 2025.

MORÁN, Alejandra. 2020. "Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera?" En: Revista del Instituto de Ciencias Jurídicas de Puebla. Vol. 15, No. 48, pp. 290-323. Disponible en línea. En: https://revistaius.com/index.php/ius/article/view/706/795. Fecha de consulta: 25 de enero de 2025.

PÉREZ, Jacinto. 2021. "Cibercriminalidad: Hacia la nueva realidad -virtual- del derecho penal" En: Revista internacional de doctrina y jurisprudencia. No. 26, pp. 175-193. Disponible en línea. En: https://ojs.ual.es/ojs/index.php/RIDJ/article/view/7063/5890. Fecha de consulta: 12 de marzo de 2025.

PRESIDENTE DE LA REPÚBLICA DEL PERÚ. 2014. Ley de Delitos Informáticos No. 30096. Disponible en línea. En: https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf. Fecha de consulta: 10 de marzo de 2025.

SARMIENTO-CHAMBA, Jose; Maldonado-Ruiz, Luis. 2024. "Delitos informáticos y ciberataques: análisis jurídico en el derecho penal del Ecuador' En: MQRInvestigar. Vol. 8, No. 3, pp. 1753-1781. Disponible en línea. En: https://doi.org/https://doi.org/10.56048/MQR20225.8.3.2024.1753-1781. Fecha de consulta: 14 de abril de 2025.

SOMMA, Alessandro. 2015. Introducción al Derecho comparado. Editorial Committee. Madrid, España. Disponible en línea. En: https://doi.org/https://www.corteidh.or.cr/tablas/r34961.pdf. Fecha de consulta: 14 de febrero de 2025.

UNIVERSIDAD DEL ZULIA

CUESTIONES POLÍTICAS

Vol.43 Nº 83

Esta revista fue editada en formato digital y publicada en agosto de 2025, por el ***Fondo Editorial Serbiluz, Universidad del Zulia. Maracaibo-Venezuela***

www.luz.edu.ve
www.serbi.luz.edu.ve
www.produccioncientificaluz.org