La Dignidad Humana frente al algoritmo: Un análisis dogmático y normativo del instrumento delictual en Colombia y México

Human Dignity in the Face of the Algorithm: A Dogmatic and Normative Analysis of the Criminal Instrument in Colombia and Mexico

Resumen

La presente investigación analiza el impacto de la Inteligencia Artificial (IA) en la configuración de conductas penalmente relevantes y su integración en el sistema judicial, mediante un estudio comparado entre Colombia y México. Se examina la génesis del ciberdelito desde la evolución histórica marcada por la Ley 1273 de 2009 y los desafíos dogmáticos que la autonomía algorítmica plantea a las categorías clásicas de la teoría del delito, tales como la noción de acción y la imputación objetiva. Asimismo, se exploran los fundamentos de la cibercriminología, basándose en la Teoría de la Transición Espacial, para comprender cómo el anonimato y la desterritorialización facilitan la criminalidad digital. El artículo evalúa la funcionalidad de herramientas predictivas como el sistema Prisma y modelos de Machine Learning, destacando su eficacia en la reducción de la impunidad, pero advirtiendo sobre el riesgo de sesgos algorítmicos. Finalmente, se concluye con la necesidad de implementar un Protocolo de Gobernanza Algorítmica (PGA) que garantice la transparencia, la equidad y la protección de los derechos fundamentales en la justicia penal de la era digital. A partir de este análisis se sostiene que el uso de la tecnología debe ser un puente hacia la eficiencia, pero nunca un muro que oculte la justicia.

Palabras clave: Cibercriminología; Ciberdelito; Derecho Penal; Gobernanza Algorítmica; Inteligencia Artificial; Política Criminal.

Abstract

This research analyzes the impact of Artificial Intelligence (AI) on the configuration of criminally relevant conduct and its integration into the judicial system through a comparative study between Colombia and Mexico. It examines the genesis of cybercrime from the historical evolution marked by Law 1273 of 2009 and the dogmatic challenges that algorithmic autonomy poses to the classical categories of the theory of crime, such as the notion of action and objective imputation. Likewise, the foundations of cybercriminology are explored, based on Space Transition Theory, to understand how anonymity and deterritorialization facilitate digital criminality. The article evaluates the functionality of predictive tools such as the Prisma system and Machine Learning models, highlighting their effectiveness in reducing impunity while warning about the risk of algorithmic biases. Finally, it concludes with the need to implement an Algorithmic Governance Protocol (AGP) that guarantees transparency, equity, and the protection of fundamental rights in criminal justice within the digital age. Based on this analysis, it is maintained that the use of technology should be a bridge to efficiency, but never a wall that obscures justice. Based on this analysis, it is maintained that the use of technology should be a bridge to efficiency, but never a wall that obscures justice.

Kewords: Algorithmic Governance; Artificial Intelligence; Cybercrime; Cybercriminology; Criminal Law; Criminal Policy.

Introducción

Es indiscutible que el uso de la IA ha permeado si bien no todas, la mayoría de las esferas de la sociedad. En este sentido, se entiende que distintas esferas del contexto económico, social y jurídico se han visto atravesados por novedosas dinámicas de interacción que exceden las conceptualizaciones y previstas en el marco normativo. En este sentido, el derecho penal enfrenta grandes retos, especialmente cuando la IA además de ser usada como una herramienta auxiliar, representa un medio potencial para la ejecución de conductas delictivas. Situación que, como manifiestan Casanova & Martín (2023), comporta una revisión profunda de las categorías jurídicas clásicas que han sustentado históricamente la teoría del delito.

Más allá de la eficiencia técnica, la presente investigación se detiene en la vulnerabilidad del sujeto procesal, recordando que el derecho penal no es solo un sistema de normas, sino una garantía de la libertad humana en relación con el error maquinal.

En todo caso, incorporar sistemas de inteligencia artificial en actividades humanas amplia las posibilidades de comisión de delitos, facilitando la automatización de conductas, la sofisticación de los mecanismos de engaño y la dificultad en la identificación de los responsables. Fenómenos como los fraudes automatizados, la suplantación de identidad a partir del uso de tecnologías de generación de contenido sintético y la suplantación de identidad a partir de tecnologías de generación de contenido sintético y la manipulación de información evidencia que la IA también puede utilizarse como instrumento altamente eficaz para la criminalidad contemporánea (Morales Moreno, 2021).

Así las cosas, Ojeda (2026) manifiesta que la inteligencia artificial plantea tensiones dogmáticas importantes en relación con los elementos estructurales del delito. En particular, la noción de acción que se entiende tradicionalmente como comportamiento humano voluntario, se cuestiona siempre que intervienen sistemas autónomos capaces de tomar decisiones sin intervención directa e inmediata de una persona. Circunstancia que obliga a replantear los fundamentos de la imputación penal, especialmente en relación con la autoría y la participación.

En este orden de ideas, Posada Maya (2017) sostiene que la teoría del delito clásica diseñada para un mundo de acciones físicas y resultados materiales resulta insuficiente para explicar la fenomenología del crimen. En concordancia, resulta pertinente argumentar de acuerdo con el autor que, la concepción del delito se encuentra frente a un nuevo paradigma delictivo que ocurre en el ciberespacio, un ámbito deslocalizado que no responde a las leyes de la física tradicional. Por tanto, se propone que la dogmática penal debe ser complementada o replanteada, toda vez que el estudio de estas conductas caracterizadas por ser automáticas, masivas y técnicas que difícilmente son atendidas a satisfacción por lo que el autor denomina la teoría del delito analógico.

Dentro de los planteamientos hechos por Posada Maya (2017) se plantea la transición hacia la ciber acción, concepto que redefine la conducta humana por su virtualidad y capacidad de programación. En el contexto del cibercrimen, la intervención humana es cada vez menos directa, permitiendo que sistemas automáticos ejecuten construcciones complejas

sin la participación física concomitante de un sujeto. Esta realidad, requiere la sustitución del nexo de casualidad tradicional por una conexión virtual o nexo lógico, donde la relación de dependencia de una instrucción informática del usuario digital, atravesada siempre por la interacción de la triada informática.

En concordancia, se destaca que asuntos como el cibercrimen requieren una re-caracterización del sujeto activo, quien no sería únicamente una persona física sino un usuario con una identidad digital que domina el tratamiento de información. En cuanto al objeto sobre el cual recae la acción se tiene que es inmaterial, lo que desplaza el interés jurídico dirigido hacia la seguridad de la información como un bien intermedio que protege la integridad, confidencialidad y disponibilidad de los datos. Análisis que concluye que la tipicidad debe evolucionar para enfrentar desafíos modernos como el anonimato facilitado por la *Deep web* y la posible responsabilidad derivada de entes autónomos de IA (Posada Maya, 2017).

Asimismo, la imputación objetiva enfrenta dificultades al tratar de establecer el nexo entre la conducta humana y el resultado lesivo cuando la inteligencia artificial interviene como intermediaria o ejecutora del hecho. La opacidad algorítmica, característica de muchos sistemas de IA, complica la previsibilidad del resultado y, en consecuencia, la determinación del riesgo jurídicamente desaprobado (Gallegos, 2022). Esto genera incertidumbre sobre los criterios tradicionales de atribución de responsabilidad.

En el ámbito de la culpabilidad, los desafíos son igualmente relevantes. La exigencia de dolo o culpa como presupuestos de la responsabilidad penal se ve tensionada cuando los resultados lesivos derivan de decisiones adoptadas por sistemas de inteligencia artificial, cuya programación puede incluir márgenes de aprendizaje autónomo (Puig, 2003). En estos casos, surge la interrogante sobre si es posible atribuir responsabilidad al programador, al usuario o incluso considerar nuevas formas de responsabilidad jurídica.

A nivel normativo, tanto Colombia como México presentan avances limitados en la regulación específica del uso de la inteligencia artificial en contextos delictivos. En ambos países, la respuesta del derecho penal ha consistido principalmente en la adaptación de tipos penales tradicionales a nuevas formas de criminalidad digital, lo que evidencia la existencia de vacíos normativos frente a las particularidades de la IA. Esta situación plantea la necesidad de evaluar la suficiencia de los marcos legales actuales (Gélvez et al, 2021).

En Colombia, si bien se han realizado esfuerzos recientes para incorporar conductas relacionadas con tecnologías emergentes dentro del ámbito penal, la regulación de la inteligencia artificial sigue siendo incipiente. Por su parte, en México, aunque existen normas orientadas a combatir la violencia digital y otros delitos tecnológicos, no se observa una regulación integral que aborde de manera específica los riesgos asociados al uso delictivo de la IA (Quiñones et al, 2025).

Este panorama normativo fragmentado refleja una problemática más amplia relacionada con la capacidad del derecho penal para adaptarse a los avances tecnológicos. La velocidad con la que evoluciona la inteligencia artificial contrasta con la rigidez inherente a los sistemas jurídicos, generando una brecha que puede ser aprovechada por actores delictivos. En este sentido, resulta fundamental analizar si las respuestas actuales son suficientes o si se requiere una reformulación más profunda del marco penal.

Desde la perspectiva de la política criminal, la inteligencia artificial también plantea interrogantes sobre las estrategias más adecuadas para prevenir y sancionar su uso indebido. La adopción de medidas exclusivamente punitivas podría resultar insuficiente frente a un fenómeno de carácter global y altamente dinámico. Por ello, se hace necesario considerar enfoques integrales que incluyan prevención, regulación tecnológica y cooperación internacional (Jímenez, 2024).

En este contexto, surge el problema de investigación que orienta el presente estudio: la insuficiencia de los marcos dogmáticos y normativos tradicionales del derecho penal para abordar adecuadamente las conductas delictivas mediadas por inteligencia artificial en Colombia y México. Este problema se manifiesta en la dificultad para imputar responsabilidad penal, la existencia de vacíos legales y la ausencia de políticas criminales articuladas frente a este fenómeno.

En atención a lo anterior, el objetivo general de esta investigación consiste en analizar el impacto del uso de la inteligencia artificial en la configuración de conductas penalmente relevantes, a partir de un estudio comparado entre Colombia y México, con el fin de identificar los desafíos dogmáticos, los vacíos normativos y las respuestas de política criminal emergentes en ambos ordenamientos jurídicos.

De manera específica, el estudio se orienta a examinar el tratamiento jurídico-penal de la inteligencia artificial en ambos países, analizar los problemas dogmáticos que esta

plantea en la teoría del delito y comparar las respuestas de política criminal adoptadas o proyectadas frente a su uso delictivo. Este enfoque permite abordar el fenómeno desde una perspectiva integral que articula distintos niveles de análisis.

Metodológicamente, la investigación se desarrolla bajo un enfoque cualitativo, utilizando como estrategia principal la revisión documental. Este método implica el análisis sistemático de fuentes normativas, doctrinales y jurisprudenciales relevantes, con el propósito de identificar tendencias, vacíos y propuestas en torno a la regulación de la inteligencia artificial en el ámbito penal.

La presente investigación emplea el uso de herramientas de IA exclusivamente para la organización de la información bibliográfica y el refinamiento de estilo, conservando la autoría y el juicio crítico del investigador en relación con las tesis dogmáticas planteadas.

La revisión documental se centra en la recopilación y análisis de legislación vigente en Colombia y México, así como en estudios académicos, artículos científicos y documentos institucionales que abordan la relación entre inteligencia artificial y derecho penal. Este proceso permite construir un marco teórico sólido y fundamentado que sustenta el análisis comparado.

Finalmente, el presente estudio busca contribuir al debate académico y jurídico sobre la necesidad de adaptar el derecho penal a los desafíos que plantea la inteligencia artificial. A través del análisis comparado entre Colombia y México, se pretende ofrecer elementos que orienten la formulación de respuestas normativas y de política criminal más eficaces, acordes con las transformaciones tecnológicas contemporáneas.

1. Génesis y fundamentos conceptuales de la Ciberdelincuencia y la Inteligencia Artificial en el Contexto Penal

1.1. Evolución Histórica y Factores Determinantes del Ciberdelito en Colombia

En la actual era digital, el acelerado desarrollo de las tecnologías de la información y las comunicaciones (TIC) ha transformado significativamente la vida de las personas, generando beneficios en la comunicación y la economía, pero también dando lugar a nuevos y complejos desafíos legales (Astaiza Morales & Cuellar Quintero, 2023). Este avance tecnológico ha facilitado el surgimiento del ciberdelito, entendido como todo acto ilegal realizado por un ciberdelincuente en el espacio digital a través de redes informáticas y

dispositivos electrónicos, con el fin de atentar contra la integridad, confidencialidad de los datos y el patrimonio económico (Astaiza Morales & Cuellar Quintero, 2023). La historia de este fenómeno es particular, pues sus orígenes se remontan a mediados de los años ochenta, mucho antes de la masificación del internet, con ataques a redes de locales comerciales (LE VPN, 2017, citado en Astaiza Morales & Cuellar Quintero, 2023).

Específicamente en Colombia, los antecedentes de los tipos penales informáticos se ubican en las décadas de mil novecientos ochenta y noventa, coincidiendo con la proliferación de la computación en el país (Astaiza Morales & Cuellar Quintero, 2023). En aquel periodo, los delitos estaban principalmente relacionados con la piratería de software y el acceso no autorizado, siendo perseguidos bajo marcos legales tradicionales, como el Código Penal de mil novecientos ochenta, que no estaban diseñados para la ciberseguridad (Astaiza Morales & Cuellar Quintero, 2023). Esta realidad obligó al legislador a crear normativas específicas para proteger el bien jurídico de la información y los datos, reconociendo que la ciberdelincuencia es un fenómeno que trasciende las fronteras físicas y legales tradicionales (Jahankhani, 2018, citado en Villegas Restrepo & Londoño Rosas, 2024).

El hito normativo más relevante en el país fue la expedición de la Ley mil doscientos setenta y tres de dos mil nueve, la cual modificó el Código Penal adicionando sanciones específicas para preservar los sistemas de tecnologías de información (Astaiza Morales & Cuellar Quintero, 2023). Esta ley tipificó conductas como la interceptación de datos, la falsificación y el daño informáticos, sentando las bases legales para enfrentar los retos de la era digital (Astaiza Morales & Cuellar Quintero, 2023). A pesar de este avance, el surgimiento del ciberdelito ha sido impulsado por factores como la expansión de la conectividad, el acceso generalizado a internet y la creciente adopción de dispositivos electrónicos (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020, citado en Astaiza Morales & Cuellar Quintero, 2023).

Otro factor determinante en la génesis de este fenómeno es la existencia de brechas de seguridad informática, tanto a nivel individual como empresarial, que permiten a los delincuentes acceder a información sensible (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020, citado en Astaiza Morales & Cuellar Quintero, 2023). Asimismo, el desarrollo de habilidades técnicas especializadas por parte de los delincuentes, tales como

el hacking, la ingeniería social y la programación maliciosa, ha sofisticado los ataques y violaciones de seguridad (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020, citado en Astaiza Morales & Cuellar Quintero, 2023). Esta evolución técnica se suma a la participación de la delincuencia organizada, que utiliza la tecnología para el fraude financiero, el tráfico de datos y el lavado de dinero a escala internacional (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020, citado en Astaiza Morales & Cuellar Quintero, 2023).

Finalmente, la internacionalización de la delincuencia permite que los actores delictivos locales se conecten con redes internacionales, facilitando la colaboración y el intercambio de conocimientos (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020, citado en Astaiza Morales & Cuellar Quintero, 2023). Esta naturaleza global del ciberespacio complica la identificación y persecución de los responsables, exigiendo una respuesta penal que no sea solo reactiva, sino proactiva y coordinada internacionalmente (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020, citado en Astaiza Morales & Cuellar Quintero, 2023). En consecuencia, el análisis de estos delitos debe considerar no solo la norma, sino las dinámicas tecnológicas que los habilitan.

El hito normativo de la ley 1273 de 2009 no fue solo una adición de tipos penales, sino la creación de un nuevo bien jurídico: la protección de la información y los datos diferenciándose del modelo anterior de 1980.

1.2. Desafíos Dogmáticos de la Inteligencia Artificial en la Teoría del Delito

La incorporación de sistemas de Inteligencia Artificial (IA) en actividades humanas ha ampliado las posibilidades de comisión de delitos, facilitando la automatización de conductas y la sofisticación de mecanismos de engaño (Morales Moreno, 2021). Fenómenos como los fraudes automatizados, la suplantación de identidad mediante contenido sintético y la manipulación de información evidencian que la IA es un instrumento altamente eficaz para la criminalidad contemporánea (Morales Moreno, 2021). Esta situación exige una revisión profunda de las categorías jurídicas clásicas que han sustentado históricamente la teoría del delito, dado que la IA desborda los marcos normativos tradicionales (Casabona & Martín, 2023).

Conforme a las afirmaciones de Hernández & López (2025) se plantea como primer desafío la crisis dentro de las categorías fundamentales en la teoría del delito, específicamente en relación con la noción de acción y la imputación objetiva. En este sentido se explica que el comportamiento humano voluntario representa la base del derecho penal tradicional y se ve cuestionado por los sistemas autónomos que toman decisiones sin la intervención humana directa. La opacidad algorítmica conocida también como el fenómeno de caja negra obstaculiza el establecimiento del nexo causal entre el programador y el resultado lesivo, lo que genera una incertidumbre sustancial al intentar determinar el riesgo jurídicamente desaprobado. Esta situación, obliga a replantear si las estructuras actuales de autoría y participación sin suficientes o si la autonomía de los algoritmos compone una barrera insalvable para la imputación penal clásica.

Ahora bien, con referencia al aspecto procesal Hernández & López (2025) explica que la implementación de herramientas predictivas como lo son el sistema prisma en Colombia pretende dotar de celeridad a la justicia, no obstante, comporta situaciones críticas de carácter ético. Pese a encontrarse el modelo *Machone Learning* que asiste en la evaluación de la probabilidad de reincidencia, existe el peligro de que sean los sesgos algorítmicos quienes perpetúen discriminaciones fundadas en factores socioeconómicos o raciales presentes en los datos históricos. Así pues, se entiende que existe una tensión directa con preceptos procesales como la presunción de inocencia, toda vez que el reporte de una máquina podría influir desproporcionalmente en la discrecionalidad del juez, principalmente en los casos en que la defensa no tiene acceso a los métodos matemáticos o medios tecnológicos para controvertir las apreciaciones de la IA que en cualquier caso es el resultado de la programación binaria de códigos.

Así entonces, se encuentra el escenario jurídico frente a un inminente riesgo de deshumanización del derecho, toda vez que la administración de justicia podría quedar relegada a la implementación de algoritmos que carecen de herramientas como la empatía y la sensibilidad propias de los seres humanos. Lo anterior, se postula partiendo de la concepción de que la labor judicial no corresponde a la aplicación automática de normas si no que representa un ejercicio de ponderación y de análisis contextual que comporta un juicio de carácter crítico que las máquinas no pueden replicar en su totalidad. En consecuencia, la pérdida del análisis de circunstancias excepcionales y factores atenuantes en una decisión

automatizada supondría un retroceso en las garantías fundamentales, por lo que la tecnología debe ser siempre un instrumento de carácter auxiliar y nunca un sustituto del razonamiento humano.

Desde una perspectiva dogmática, la IA plantea tensiones significativas sobre la noción de acción, tradicionalmente entendida como un comportamiento humano voluntario (Ojeda, 2026). Cuando intervienen sistemas autónomos capaces de tomar decisiones sin intervención humana directa e inmediata, se pone en duda la base de la imputación penal y los criterios clásicos de autoría y participación (Ojeda, 2026). El análisis se centra ahora en determinar si estas conductas pueden seguir atribuyéndose exclusivamente a un individuo o si la autonomía algorítmica crea una barrera insalvable para el derecho penal tradicional.

Por otro lado, la imputación objetiva enfrenta dificultades para establecer el nexo entre la conducta humana y el resultado lesivo cuando la IA interviene como intermediaria o ejecutora. La opacidad algorítmica, característica de muchos sistemas de aprendizaje profundo, complica la previsibilidad del resultado y, por ende, la determinación del riesgo jurídicamente desaprobado (Gallegos, 2022). Esta "caja negra" tecnológica genera una incertidumbre sustancial sobre los criterios de atribución de responsabilidad que el sistema judicial aún intenta descifrar.

En el ámbito de la culpabilidad, la exigencia de dolo o culpa se ve tensionada cuando los resultados lesivos derivan de decisiones adoptadas por sistemas con márgenes de aprendizaje autónomo (Puig, 2003). Surge entonces la interrogante de si es posible atribuir responsabilidad penal al programador, al usuario final o si deben considerarse nuevas formas de responsabilidad jurídica para estas entidades tecnológicas (Puig, 2003,). Ante este panorama fragmentado, resulta fundamental evaluar si los marcos legales actuales de Colombia son suficientes para abordar conductas mediadas por algoritmos (Gélvez et al, 2021).

La respuesta del derecho penal ha consistido principalmente en la adaptación de tipos penales tradicionales a nuevas formas de criminalidad digital, lo que evidencia la existencia de vacíos normativos (Gélvez et al, 2021). La velocidad de la evolución tecnológica contrasta con la rigidez de los sistemas jurídicos, creando brechas que son aprovechadas por actores delictivos (Quiñones et al, 2025). Por ello, la política criminal no puede limitarse a medidas

exclusivamente punitivas, sino que requiere enfoques integrales que incluyan regulación tecnológica y cooperación internacional (Jímenez, 2024).

1.3. Cibercriminología, Principios y el Paradigma de la Prevención Predictiva

La cibercriminología surge como una rama especializada para estudiar los delitos cometidos en el ciberespacio, comprendiendo cómo sus características únicas influyen en el comportamiento (Jaishankar, 2008, citado en Villegas Restrepo & Londoño Rosas, 2024). Un fundamento esencial es la Teoría de la Transición Espacial, la cual propone que el ciberespacio crea un entorno que altera las normas sociales y las restricciones del mundo físico (Jaishankar, 2008, citado en Villegas Restrepo & Londoño Rosas, 2024). Según esta teoría, las personas se comportan de forma distinta al transicionar al espacio digital debido al anonimato y la falta de controles sociales directos, lo que reduce el miedo a la sanción (Jaishankar, 2008, citado en Villegas Restrepo & Londoño Rosas, 2024).

Las interacciones digitales también pueden llevar a la desinhibición, fomentando conductas desviadas que no se manifestarían en el contacto cara a cara (Suler, 2004, citado en Villegas Restrepo & Londoño Rosas, 2024). Esta dinámica psicológica, sumada a una estructura social donde los controles formales son menos efectivos, facilita que los delincuentes operen en múltiples jurisdicciones (Jaishankar, 2008, citado en Villegas Restrepo & Londoño Rosas, 2024). En consecuencia, la cibercriminología debe analizar no solo los aspectos técnicos, sino los contextos sociales que fomentan el cibercrimen (Holt & Bossler, 2020, citado en Villegas Restrepo & Londoño Rosas, 2024).

El fenómeno se rige por principios como la desterritorialización, donde los delitos trascienden los límites geográficos tradicionales (Clough, 2010, citado en Villegas Restrepo & Londoño Rosas, 2024). Otro principio clave es la asimetría de la información y el poder, donde individuos con altos conocimientos técnicos pueden ejercer un impacto desproporcionado sobre grandes corporaciones o infraestructuras críticas (Dunne, 2009, citado en Villegas Restrepo & Londoño Rosas, 2024). Esta asimetría redefine el poder en el contexto criminal, permitiendo que un solo actor cause daños masivos (Dunne, 2009, citado en Villegas Restrepo & Londoño Rosas, 2024).

La escalabilidad permite que los ciberdelitos se expandan rápidamente con un esfuerzo mínimo, logrando impactos globales en cuestión de horas (Clough, 2010, citado en Villegas Restrepo & Londoño Rosas, 2024). Asimismo, la persistencia y evolución subraya

que los atacantes adaptan continuamente sus métodos para evadir medidas de seguridad (Dunne, 2009, citado en Villegas Restrepo & Londoño Rosas, 2024). Por otro lado, la materialidad virtual resalta que, aunque ocurran en el entorno digital, los impactos son reales, causando pérdidas financieras y daños psicológicos tangibles (Mesa, 2020, citado en Villegas Restrepo & Londoño Rosas, 2024).

Frente a esta complejidad, surge la criminología computacional y el predictive policing como herramientas de vanguardia (Ramírez Pérez, 2025). El uso de modelos de Machine Learning (ML) permite identificar patrones no lineales y predecir puntos calientes o hotspots de criminalidad, optimizando los recursos del Estado (Muñoz Jaramillo, 2021, citado en Ramírez Pérez, 2025). Sin embargo, esto plantea desafíos éticos como el sesgo de retroalimentación (Feedback Bias), que puede perpetuar la discriminación algorítmica si no existe una supervisión crítica (Lum & Isaac, 2016, citado en Ramírez Pérez, 2025).

En Colombia, se han propuesto sistemas como Prisma (Perfil de Riesgo de Reincidencia), que utiliza el aprendizaje supervisado para predecir la probabilidad de que un individuo vuelva a delinquir (Díaz-Rincón et al., 2024). Esta herramienta busca apoyar a los jueces de control de garantías, aportando celeridad y reduciendo la percepción de impunidad (Díaz-Rincón et al., 2024). No obstante, su uso genera cuestionamientos sobre la transparencia y el derecho a la defensa, ya que los defensores a menudo desconocen el método matemático detrás de los reportes (Pagallo & Quattrocolo, 2018, citado en Díaz-Rincón et al., 2024).

La ética en el uso de estas tecnologías exige que el criterio humano prevalezca en las decisiones judiciales (Khan et al., 2023, citado en Díaz-Rincón et al., 2024). La Corte Constitucional en la Sentencia T-trescientos veintitrés de dos mil veinticuatro ha señalado que la IA debe ser un instrumento auxiliar y no sustitutivo de la labor del juez (Díaz-Rincón et al., 2024). La justicia penal debe, por tanto, integrar la analítica de datos sin abandonar los principios de racionalidad y proporcionalidad (Díaz-Rincón et al., 2024).

Finalmente, la transición hacia una gobernanza algorítmica transparente es imperativa para garantizar la seguridad nacional y ciudadana (Ramírez Pérez, 2025). El reto para el futuro cercano será consolidar modelos predictivos que no solo sean técnicamente precisos, sino éticamente legítimos, incorporando variables socioestructurales que fundamenten la inversión social y no solo la respuesta punitiva (Ramírez Pérez, 2025). Solo así el Estado

podrá enfrentar eficazmente las amenazas de la era digital respetando los derechos fundamentales (Villegas Restrepo & Londoño Rosas, 2024).

La materialidad virtual no debe desconocer de ningún modo que detrás de cada dato alterado hay una víctima de daños materiales reales, lo que exige que la justicia a demás de identificar patrones restaure la confianza ciudadana. En consecuencia, la caja negra a la que se analiza desde un punto de vista crítico es la misma que se evita en este estudio exponiendo de forma clara y auditable el razonamiento jurídico utilizado.

2. Mecanismos normativos de protección y regulación del ciberdelito

2.1. Mecanismos Normativos de Protección y Regulación del Ciberdelito

El ordenamiento jurídico colombiano ha respondido de manera progresiva a los desafíos impuestos por la delincuencia informática, estableciendo mecanismos que buscan prevenir, investigar y sancionar conductas que atentan contra la seguridad de la información. El pilar fundamental de esta respuesta es la Ley mil doscientos setenta y tres de dos mil nueve, la cual introdujo un nuevo bien jurídico tutelado: la protección de la información y de los datos (Astaiza Morales & Cuellar Quintero, 2023). Esta normativa modificó el Código Penal para tipificar delitos que no existían anteriormente, reconociendo que el avance de las tecnologías de la información y la comunicación (TIC) exigía un tratamiento legal especializado frente a conductas como la interceptación de datos y el daño informático (Astaiza Morales & Cuellar Quintero, 2023).

Complementando este marco, la Ley quince mil ochocientos uno de dos mil doce, conocida como Ley de Protección de Datos Personales, aunque no es de carácter estrictamente penal, constituye un mecanismo de protección preventivo esencial (Astaiza Morales & Cuellar Quintero, 2023). Su objetivo es garantizar el derecho constitucional a la privacidad, regulando el tratamiento de la información en medios digitales y telemáticos, lo que contribuye a reducir la superficie de ataque para los delincuentes (Astaiza Morales & Cuellar Quintero, 2023). Ambas leyes forman un ecosistema normativo que busca armonizar la legislación nacional con estándares internacionales, facilitando la persecución de delitos que, por su naturaleza, suelen ser transnacionales (Villegas Restrepo & Londoño Rosas, 2024).

A pesar de contar con estas leyes, la efectividad de la política criminal en Colombia se ha visto limitada por la velocidad de la evolución tecnológica, que a menudo supera la capacidad de actualización legislativa (Pérez, Rodríguez, Flórez & Martínez, 2010, citado en Astaiza Morales & Cuellar Quintero, 2023). Factores como la expansión de la conectividad y la adopción masiva de dispositivos electrónicos han brindado a los delincuentes plataformas más amplias para el fraude y la extorsión (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020, citado en Astaiza Morales & Cuellar Quintero, 2023). En este sentido, la ley debe ser entendida como un instrumento dinámico que requiere reajustes constantes en su redacción para evitar que las defensas técnicas aprovechen vacíos metodológicos (Astaiza Morales & Cuellar Quintero, 2023).

La internacionalización de la delincuencia es otro factor que presiona el marco normativo actual, ya que los delincuentes locales operan bajo el anonimato que ofrecen las redes globales, conectándose con grupos organizados en diferentes jurisdicciones (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020, citado en Astaiza Morales & Cuellar Quintero, 2023). Este fenómeno dificulta la individualización de los responsables y exige una cooperación internacional robusta, como la que promueve el Convenio de Budapest, ratificado por Colombia mediante la Ley mil novecientos veintiocho de dos mil dieciocho (Villegas Restrepo & Londoño Rosas, 2024). Sin embargo, existe un desfase entre la adhesión a tratados y la implementación de capacidades técnicas en la policía judicial para recolectar evidencia digital efectiva (Villegas Restrepo & Londoño Rosas, 2024).

Desde el punto de vista de la política pública, se han emitido documentos CONPES orientados a fortalecer la ciberseguridad y la confianza digital, como el CONPES tres mil novecientos noventa y cinco de dos mil veinte (Villegas Restrepo & Londoño Rosas, 2024). No obstante, estos documentos a menudo carecen de fuerza vinculante, lo que genera una aplicación inconsistente de las estrategias preventivas en las diferentes entidades del Estado (Villegas Restrepo & Londoño Rosas, 2024). La falta de una política criminal integral que articule la prevención situacional con la respuesta punitiva ha llevado a que el sistema penal opere de forma reactiva, basándose en un "modelo penal del castigo" que no reduce la incidencia delictiva a largo plazo (Ramírez Pérez, 2025).

La pedagogía jurídica se identifica como una herramienta de protección no normativa fundamental que el Estado debe fomentar para reducir la vulnerabilidad de los ciudadanos

(Molina, 2010, citado en Astaiza Morales & Cuellar Quintero, 2023). Muchos ciberataques tienen éxito debido al desconocimiento de medidas básicas de ciberseguridad, lo que convierte a la población en un "blanco fácil" para técnicas de ingeniería social (Astaiza Morales & Cuellar Quintero, 2023). Por tanto, la protección del bien jurídico de la información no solo depende de la sanción penal, sino de un esfuerzo colectivo que incluya a la academia y al sector privado en la creación de una cultura de prevención (Villegas Restrepo & Londoño Rosas, 2024).

Finalmente, el incremento en la denuncia de delitos como el acceso abusivo a sistemas informáticos —que reportó un alza del cuarenta y seis por ciento en periodos recientes— evidencia que la ley mil doscientos setenta y tres de dos mil nueve es más necesaria que nunca (Lorduy, 2022, citado en Astaiza Morales & Cuellar Quintero, 2023). La justicia penal debe comprometerse a invertir en tecnologías de punta para la Fiscalía General de la Nación, asegurando que la persecución de estos criminales no sea solo un ideal normativo, sino una realidad operativa (Astaiza Morales & Cuellar Quintero, 2023). El reto institucional reside en cerrar la brecha entre la norma escrita y la capacidad técnica para materializarla en sentencias condenatorias (Astaiza Morales & Cuellar Quintero, 2023).

En conclusión, los mecanismos normativos vigentes en Colombia ofrecen una estructura base sólida, pero enfrentan desafíos estructurales derivados de la asimetría tecnológica (Villegas Restrepo & Londoño Rosas, 2024). Solo mediante la integración de la analítica de datos, la actualización legislativa y la cooperación internacional, el Estado podrá ofrecer una protección efectiva frente a la criminalidad de la era digital (Ramírez Pérez, 2025).

2.2. Análisis Dogmático y Funcionalidad de la IA en el Proceso Penal

El análisis dogmático de los tipos penales informáticos en Colombia requiere un estudio detallado de la tipicidad objetiva y subjetiva de las conductas consagradas entre los artículos doscientos sesenta y nueve A y doscientos sesenta y nueve J del Código Penal (Astaiza Morales & Cuellar Quintero, 2023). La mayoría de estos delitos se configuran como delitos de acción y, en muchos casos, de peligro, donde el mero acceso no autorizado a un sistema informático ya constituye una afectación al bien jurídico (Astaiza Morales & Cuellar Quintero, 2023). Por ejemplo, el acceso abusivo a un sistema informático (Art. doscientos sesenta y nueve A) no requiere un resultado material lesivo inmediato para ser punible,

bastando con superar las medidas de seguridad sin voluntad del administrador (Astaiza Morales & Cuellar Quintero, 2023).

En el ámbito de la imputación objetiva, es crucial demostrar el nexo entre la creación de un riesgo jurídicamente desaprobado y el resultado producido (Ámbito Jurídico, 2021, citado en Astaiza Morales & Cuellar Quintero, 2023). Los ciberdelincuentes suelen poseer conocimientos técnicos avanzados que les permiten crear riesgos que un ciudadano promedio no podría generar ni mitigar, lo que facilita la atribución de responsabilidad (Astaiza Morales & Cuellar Quintero, 2023). No obstante, la intencionalidad dolosa es una característica transversal en estas conductas, ya que el uso de herramientas como malware o scripts requiere plena conciencia del daño que se pretende causar a la integridad o confidencialidad de los datos (Astaiza Morales & Cuellar Quintero, 2023).

La Inteligencia Artificial (IA) ha comenzado a integrarse en el sistema penal colombiano no solo como objeto de delito, sino como herramienta de gestión judicial. Un ejemplo relevante es el sistema Prisma (Perfil de Riesgo de Reincidencia), diseñado por la Fiscalía para evaluar la probabilidad de que un indiciado vuelva a delinquir (Díaz-Rincón et al., 2024). Prisma utiliza modelos de Machine Learning (ML) supervisado que analizan variables como antecedentes penales y características del evento criminal para emitir reportes que asistan a los jueces en la imposición de medidas de aseguramiento (Fiscalía General de la Nación, 2020, citado en Díaz-Rincón et al., 2024). Esta integración busca dotar de celeridad al proceso penal y reducir la percepción de impunidad en delitos de alta recurrencia como el hurto (Díaz-Rincón et al., 2024).

Desde el punto de vista funcional, los jueces de control de garantías y de conocimiento en ciudades como Barranquilla han mostrado posiciones divergentes frente al uso de la IA (Díaz-Rincón et al., 2024). Mientras algunos reconocen que estas herramientas permiten descongestionar despachos y organizar la información de manera eficiente, otros mantienen un escepticismo razonable sobre su confiabilidad y utilidad al momento de proferir decisiones que limitan la libertad (Díaz-Rincón et al., 2024). La Corte Constitucional, en la Sentencia T-trescientos veintitrés de dos mil veinticuatro, ha sido enfática al señalar que la IA debe ser un instrumento auxiliar y que la responsabilidad sustancial de la decisión judicial debe recaer exclusivamente en el pensamiento humano del juez (Díaz-Rincón et al., 2024).

El uso de sistemas como Prisma plantea riesgos de subjetivismo y sesgos algorítmicos, ya que los modelos pueden penalizar a individuos basándose en factores socioeconómicos o demográficos que no necesariamente guardan una relación causal con su peligrosidad individual (Aguilar, 2024, citado en Díaz-Rincón et al., 2024). Esto genera una tensión con el principio de presunción de inocencia, ya que el reporte del sistema podría influir de manera desproporcionada en la discrecionalidad del juez si este no cuenta con la capacidad crítica para interpretar el método matemático subyacente (Díaz-Rincón et al., 2024). Además, la opacidad de estos sistemas —a menudo considerados "cajas negras"— limita la capacidad de la defensa para controvertir la validez del reporte técnico (Pagallo & Quattrocolo, 2018, citado en Díaz-Rincón et al., 2024).

La transferencia no consentida de activos (Art. doscientos sesenta y nueve J) se destaca como uno de los delitos más graves y concurrentes, dada su gran repercusión económica y la sofisticación necesaria para su ejecución (Astaiza Morales & Cuellar Quintero, 2023). Este tipo penal incorpora un ingrediente normativo específico: el ánimo de lucro (Astaiza Morales & Cuellar Quintero, 2023). Al ser una conducta que a menudo utiliza manipulación informática automatizada, la atribución de culpabilidad se vuelve compleja, especialmente cuando los algoritmos de IA son los que ejecutan las transacciones de forma autónoma (Astaiza Morales & Cuellar Quintero, 2023).

La ética en el uso de la IA judicial exige que cualquier implementación tecnológica respete los derechos fundamentales a la intimidad y al debido proceso (Khan et al., 2023, citado en Díaz-Rincón et al., 2024). El Gobierno Nacional ha propuesto un Marco Ético para la IA en Colombia, que enfatiza la necesidad de transparencia, seguridad jurídica y el acceso igualitario a la tecnología (Gobierno Nacional, 2021, citado en Díaz-Rincón et al., 2024). Sin embargo, la implementación práctica de estos principios en las audiencias de medidas de aseguramiento aún requiere de protocolos más claros que garanticen la contradicción probatoria (Díaz-Rincón et al., 2024).

En síntesis, la dogmática penal colombiana se encuentra en una fase de transición donde los conceptos clásicos de autoría y tipicidad deben dialogar con herramientas algorítmicas que pretenden optimizar la justicia (Díaz-Rincón et al., 2024). El éxito de esta transición dependerá de que la tecnología sirva a los fines de la resocialización y la justicia,

y no como un mecanismo de discriminación automatizada o una forma de eludir las responsabilidades sustanciales de la administración de justicia (Ramírez Pérez, 2025).

Por ende, es imperativo transitar del populismo punitivo hacia una inversión social que atienda la pobreza y la marginalidad, factores que el algoritmo derecta pero que solamente la voluntad humana puede solucionar.

2.3. Eficacia de la Política Criminal y el Horizonte de la Criminología Computacional

La eficacia del marco normativo colombiano frente al ciberdelito puede evaluarse a través de la relación entre el número de denuncias recibidas y las capturas efectuadas. El promedio nacional del índice de capturas sobre denuncias para delitos informáticos ha sido reportado en un siete punto uno por ciento, una cifra significativamente menor en comparación con el veintidós punto ocho por ciento de delitos tradicionales como el hurto calificado (Banca & Economía, 2022, citado en Astaiza Morales & Cuellar Quintero, 2023). Esta brecha sugiere una deficiencia notable en la aplicación de la ley, que puede atribuirse a la falta de recursos técnicos, el conocimiento insuficiente de los operadores judiciales o el propio anonimato que ofrece la red (Astaiza Morales & Cuellar Quintero, 2023).

Frente a esta crisis de efectividad, la criminología computacional emerge como el paradigma necesario para transitar hacia un Servicio de Policía Basado en la Evidencia (EBP) (Ramírez Pérez, 2025). Este enfoque propone utilizar el Big Data para identificar patrones delictivos no lineales y predecir puntos calientes o hotspots con mayor precisión que los métodos estadísticos tradicionales (Borges et al., 2018, citado en Ramírez Pérez, 2025). Algoritmos de aprendizaje por conjuntos como Random Forest y XGBoost han demostrado niveles de exactitud de hasta el ochenta y seis por ciento en entornos urbanos complejos como Medellín, permitiendo una asignación más eficiente de patrullaje y recursos (Muñoz Jaramillo, 2021, citado en Ramírez Pérez, 2025).

Sin embargo, el uso de analítica predictiva en seguridad ciudadana conlleva riesgos éticos, siendo el más crítico el sesgo de retroalimentación (Feedback Bias) (Lum & Isaac, 2016, citado en Ramírez Pérez, 2025). Este riesgo ocurre cuando los algoritmos se entrenan con datos históricos que reflejan sesgos previos de la vigilancia policial en zonas vulnerables, lo que lleva al sistema a predecir crímenes en las mismas áreas y reforzar una vigilancia desproporcionada (Ramírez Pérez, 2025). Para evitar una "pseudo-legitimación algorítmica",

es imperativo establecer un Protocolo de Gobernanza Algorítmica (PGA) que garantice la transparencia y la rendición de cuentas de estos modelos (Ramírez Pérez, 2025).

La Prevención Situacional del Delito (PSD), que busca reducir las oportunidades delictivas mediante la gestión del ambiente, ha sido criticada por ignorar las raíces socioestructurales de la criminalidad (Joao & Fernández Romo, 2018, citado en Ramírez Pérez, 2025). Si el Machine Learning se utiliza únicamente para el control policial sin considerar variables como la pobreza multidimensional y el desempleo, se corre el riesgo de criminalizar la marginalidad en lugar de prevenir el delito (Ramírez Pérez, 2025). Por tanto, la analítica predictiva debe fundamentar también la inversión social en educación y empleo en zonas de alto riesgo criminógeno (Ramírez Pérez, 2025).

En ciudades intermedias como Bucaramanga, la viabilidad técnica de estos modelos se ve limitada por el "escaso acervo de información delictiva georreferenciada", lo que reduce la sensibilidad de los modelos predictivos (Gélvez-Ferreira et al., 2022, citado en Ramírez Pérez, 2025). Esta realidad subraya la necesidad de fortalecer la capacidad de recolección de datos locales y centralizar la información a través de un Data Hub nacional que integre registros del SIEDCO, el RNMC y el DANE (Ramírez Pérez, 2025). Solo con datos limpios y estandarizados es posible desarrollar modelos confiables que no perpetúen injusticias sistémicas (Ramírez Pérez, 2025).

La reconfiguración del delito ante el avance de las TIC ha generado un aumento en el cibercrimen económico con una alta "cifra negra", debido a que muchas víctimas no denuncian por desconfianza en el sistema o vergüenza (González Uriel, 2024, citado en Ramírez Pérez, 2025). La política criminal debe, por ende, priorizar la formación continua de los cuerpos de policía en ciberseguridad y forense digital, adaptando los currículos educativos a las nuevas modalidades de estafa y fraude automatizado (Ávila-Niño & Rincón-Núñez, 2023, citado en Ramírez Pérez, 2025). La creación de centros de fusión interagenciales es vital para coordinar la investigación penal y afectar las estructuras financieras de los grupos delincuenciales (Ramírez Pérez, 2025).

Hacia el futuro, la hoja de ruta para el periodo dos mil veinticinco-dos mil treinta debe formalizar el tránsito hacia un modelo de Patrullaje Basado en Riesgo (PBR) (Ramírez Pérez, 2025). Este modelo debe utilizar predicciones algorítmicas no para sustituir el criterio humano, sino para optimizar la toma de decisiones en microterritorios, siempre bajo una

supervisión ética estricta (Ramírez Pérez, 2025). La efectividad de estas herramientas dependerá de que el Estado colombiano logre superar el populismo punitivo reactivo y apueste por una justicia criminal basada en datos rigurosos y principios de equidad (Ramírez Pérez, 2025).

En conclusión, el panorama del derecho penal frente al cibercrimen y la IA en Colombia revela una necesidad urgente de modernización tanto técnica como ética (Díaz-Rincón et al., 2024). La integración de la analítica predictiva ofrece una oportunidad histórica para reducir la impunidad, siempre que se ejerza dentro de un marco de gobernanza algorítmica transparente que proteja los derechos fundamentales de todos los ciudadanos (Ramírez Pérez, 2025). El éxito en la lucha contra la cibercriminalidad dependerá de la capacidad de la sociedad para armonizar la innovación tecnológica con los valores esenciales de justicia y dignidad humana (Villegas Restrepo & Londoño Rosas, 2024).

3. Funcionalidad, resultados y gobernanza de la inteligencia artificial en la prevención y persecución del delito

3.1. Funcionalidad de la IA y el sistema prisma en el Ámbito judicial Colombiano

La integración de la inteligencia artificial (IA) en el proceso penal colombiano ha pasado de ser una proyección teórica a una herramienta operativa con el objetivo de dotar de celeridad a la administración de justicia (Díaz-Rincón et al., 2024). El sistema penal enfrenta retos históricos relacionados con la lentitud en los trámites, la notificación y la práctica de pruebas, lo que ha generado una pérdida de confianza ciudadana (Gupta et al., 2023, citado en Díaz-Rincón et al., 2024). Ante este panorama, el uso de herramientas tecnológicas busca reducir la percepción de injusticia e impunidad al permitir que los trámites se produzcan en un menor tiempo en comparación con los métodos tradicionales de gestión (Díaz-Rincón et al., 2024).

Un instrumento central en esta transición es el sistema Prisma (Perfil de Riesgo de Reincidencia), diseñado por la Fiscalía General de la Nación para conocer la probabilidad de que un indiciado vuelva a delinquir (Fiscalía General de la Nación, 2020, citado en Díaz-Rincón et al., 2024). Este sistema utiliza modelos de aprendizaje supervisado (Machine Learning) que analizan características del individuo, su historia criminal y las variables del último evento delictivo (Díaz-Rincón et al., 2024). El propósito de Prisma es servir de apoyo

a los jueces de control de garantías para decretar medidas de aseguramiento, fundamentando la necesidad de la privación de libertad en casos donde el sujeto represente un peligro real para la sociedad (Díaz-Rincón et al., 2024).

La funcionalidad de Prisma se basa en reportes del Sistema Penal Oral Acusatorio (SPOA), integrando información de la Policía y otras autoridades de control para identificar la contingencia en la reiteración delictiva (Fiscalía General de la Nación, 2020, citado en Díaz-Rincón et al., 2024). Al introducir datos de individualización, el operador judicial recibe métricas que oscilan en un rango de 0 a 100, facilitando una decisión más acertada y técnica (Díaz-Rincón et al., 2024). No obstante, el sistema no pretende sustituir el criterio humano, sino actuar como una herramienta facilitadora para manejar los limitados espacios carcelarios de forma más proporcional (Fiscalía General de la Nación, 2019, citado en Díaz-Rincón et al., 2024).

Los resultados de investigaciones realizadas en ciudades como Barranquilla revelan posiciones divergentes entre los administradores de justicia respecto a la utilidad de estas herramientas (Díaz-Rincón et al., 2024). Durante el año 2022, se evidenció que los jueces de control de garantías recibieron un alto volumen de solicitudes de medidas de aseguramiento en casos de hurto, concediendo solo una parte de ellas tras evaluar la incidencia de la IA en la solicitud (Díaz-Rincón et al., 2024). Mientras que los jueces de conocimiento tienden a ver la IA como un factor favorable para la organización de la información, existe un escepticismo persistente sobre su confiabilidad absoluta al momento de limitar derechos fundamentales (Díaz-Rincón et al., 2024).

El uso de la IA en el sistema penal también enfrenta límites críticos en materia de transparencia y derecho a la defensa (Díaz-Rincón et al., 2024). Dado que Prisma no es una base de datos pública y contiene información reservada, los defensores a menudo se encuentran en una posición de desigualdad al no poder controvertir el método matemático que sustenta el reporte (Pagallo & Quattrocolo, 2018, citado en Díaz-Rincón et al., 2024). Esta opacidad algorítmica genera desconcierto y puede limitar la controversia probatoria, exigiendo que la Fiscalía suministre explicaciones argumentativas detalladas y no se limite a alegar un resultado automático (Díaz-Rincón et al., 2024).

Desde un enfoque metodológico, el estudio de este fenómeno en Colombia ha adoptado paradigmas fenomenológicos para comprender cómo la superposición de la

tecnología afecta la humanización de las decisiones judiciales (Husserl, 1993, citado en Díaz-Rincón et al., 2024). La transición del sistema tradicional al tecnológico-virtual requiere no solo de infraestructura, sino de una adaptación institucional que garantice la seguridad de las partes en conflicto (Gupta et al., 2023, citado en Díaz-Rincón et al., 2024). El reto actual consiste en evitar que el sistema Prisma se convierta en un mecanismo de discriminación automatizada basado en factores demográficos o socioeconómicos (Aguilar, 2024, citado en Díaz-Rincón et al., 2024).

Por otro lado, la Corte Constitucional, en la Sentencia T-323 de 2024, ha establecido límites claros, señalando que la IA debe usarse solo para tareas accesorias como sintetizar información o agendar actividades (Díaz-Rincón et al., 2024). La responsabilidad sustancial de juzgar y aplicar principios de proporcionalidad y razonabilidad es exclusiva del pensamiento humano, el cual no puede ser sustituido por robots (Díaz-Rincón et al., 2024). De esta manera, el sistema Prisma impacta positivamente en la celeridad, pero su uso debe ser cauteloso para no vulnerar la presunción de inocencia de los ciudadanos (Díaz-Rincón et al., 2024).

En conclusión, la IA en el sistema judicial colombiano representa un avance significativo hacia la modernización, pero su éxito depende de la capacidad del Estado para garantizar un equilibrio entre eficiencia y derechos (Díaz-Rincón et al., 2024). La adopción tecnológica debe ser un proceso de integración que mejore la calidad de vida y la justicia, reconociendo que la tecnología es un medio para alcanzar un fin superior: el respeto por la dignidad humana (DNP, Conpes 4023 de 2021, citado en Díaz-Rincón et al., 2024).

II. Eficacia de los Modelos Predictivos y la Criminología Computacional

La eficacia del marco normativo frente al ciberdelito en Colombia puede medirse a través de la razón entre capturas y denuncias, revelando un desempeño institucional significativamente bajo en comparación con los delitos tradicionales (Banca & Economía, 2022, citado en Astaiza Morales & Cuellar Quintero, 2023). Mientras que el hurto calificado reporta un índice de capturas nacional del 22.8%, los delitos informáticos apenas alcanzan un 7.1% (Banca & Economía, 2022, citado en Astaiza Morales & Cuellar Quintero, 2023). Esta brecha sugiere una deficiencia en la efectividad de la Ley 1273 de 2009, posiblemente vinculada a la falta de recursos técnicos y capacitación especializada en la policía judicial (Banca & Economía, 2022, citado en Astaiza Morales & Cuellar Quintero, 2023).

Ante esta crisis de efectividad, la criminología computacional surge como la herramienta idónea para transitar hacia un Servicio de Policía Basado en la Evidencia (EBP) (Ramírez Pérez, 2025). Los modelos de Machine Learning son particularmente adecuados para capturar la complejidad y los patrones no lineales de la delincuencia urbana, superando las limitaciones de los métodos estadísticos tradicionales (Muñoz Jaramillo, 2021, citado en Ramírez Pérez, 2025). Algoritmos como Random Forest (RF) y Extreme Gradient Boosting (XGBoost) han demostrado altos niveles de precisión en la identificación de hotspots o puntos calientes de criminalidad (Kshatri et al., 2021, citado en Ramírez Pérez, 2025).

En entornos urbanos complejos como Medellín, el uso de estos modelos ha permitido predecir delitos como el hurto y el homicidio con niveles de exactitud de hasta el 86% (Muñoz Jaramillo, 2021, citado en Ramírez Pérez, 2025). La granularidad de los datos, analizados a nivel de barrio y grillas espaciales, facilita una asignación de recursos más eficiente y proactiva (Mohler et al., 2015, citado en Ramírez Pérez, 2025). Sin embargo, en ciudades intermedias como Bucaramanga, la viabilidad técnica disminuye debido al limitado acervo de información georreferenciada disponible (Gélvez-Ferreira et al., 2022, citado en Ramírez Pérez, 2025).

Un aspecto crucial de la criminología computacional es el modelado temporal mediante arquitecturas de Deep Learning como las redes LSTM (Long Short-Term Memory) (Safat et al., 2021, citado en Ramírez Pérez, 2025). Estas redes permiten realizar pronósticos de criminalidad (crime forecasting) capturando patrones estacionales y tendencias evolutivas en series de tiempo (Safat et al., 2021, citado en Ramírez Pérez, 2025). No obstante, la opacidad inherente a estas "cajas negras" tecnológicas plantea desafíos para su validación institucional y supervisión humana (Ramírez Pérez, 2025).

La investigación también destaca la necesidad de integrar variables criminógenas estructurales en los modelos predictivos para evitar un enfoque meramente punitivo (Ardila Chávarro, 2023, citado en Ramírez Pérez, 2025). Factores como el desempleo, la pobreza multidimensional y la desigualdad económica tienen un alto poder predictivo sobre la incidencia delictiva (Ardila Chávarro, 2023, citado en Ramírez Pérez, 2025). Si el Machine Learning omite estas variables, se corre el riesgo de criminalizar microterritorios vulnerables sin atender las raíces sociales que alimentan la violencia (Joao & Fernández Romo, 2018, citado en Ramírez Pérez, 2025).

La reconfiguración del delito ante el avance de las TIC ha incrementado el cibercrimen económico, caracterizado por una alta "cifra negra" de casos no denunciados (González Uriel, 2024, citado en Ramírez Pérez, 2025). La analítica predictiva resulta indispensable para la detección temprana de fraudes y estafas en el sector financiero, donde los algoritmos pueden identificar comportamientos anómalos en grandes volúmenes de transacciones (Rincón-Núñez, 2023, citado en Ramírez Pérez, 2025). No obstante, la policía nacional requiere una modernización urgente en ciberseguridad y forense digital para enfrentar estas modalidades sofisticadas (Ávila-Niño & Rincón-Núñez, 2023, citado en Ramírez Pérez, 2025).

A pesar de los avances, existen límites normativos y operativos que frenan el alcance de estas tecnologías. El anonimato que ofrece el ciberespacio dificulta la individualización de los responsables, convirtiendo a algunos delitos informáticos en actos prácticamente imposibles de procesar (Astaiza Morales & Cuellar Quintero, 2023). Además, la falta de jueces especializados y la sobrecarga administrativa en la rama judicial complican la culminación exitosa de los procesos iniciados mediante herramientas tecnológicas (Astaiza Morales & Cuellar Quintero, 2023).

En conclusión, la criminología computacional ofrece un potencial sin precedentes para mejorar la seguridad ciudadana, siempre que su aplicación esté guiada por datos limpios y estandarizados (Muñoz Jaramillo, 2021, citado en Ramírez Pérez, 2025). La integración de bases de datos como SIEDCO, RNMC y DANE en un Data Hub nacional es una tarea prioritaria para superar las brechas de información y construir modelos verdaderamente confiables (Ramírez Pérez, 2025). La meta debe ser transitar de una reacción policial intuitiva a una estrategia de anticipación científica que proteja los bienes jurídicos de forma equitativa (Ramírez Pérez, 2025). El éxito de la IA en la justicia no se mide en sentencias rápidas, sino en sentencias justas donde el pensamiento del juez haya ponderado el contexto humano de cada indiciado.

3.2. Gobernanza algorítmica, desafíos éticos y hoja de ruta 2025-2030

La implementación de la inteligencia artificial en la seguridad ciudadana demanda una gobernanza algorítmica que asegure la transparencia, la proporcionalidad y la equidad en la intervención estatal (Sarzaeim et al., 2023, citado en Ramírez Pérez, 2025). El riesgo ético más prominente es el sesgo de retroalimentación (Feedback Bias), el cual ocurre cuando

los algoritmos se entrenan con datos históricos que reflejan sesgos policiales previos en zonas estigmatizadas (Lum & Isaac, 2016, citado en Ramírez Pérez, 2025). Este fenómeno puede perpetuar un ciclo de vigilancia desproporcionada sobre comunidades vulnerables, amplificando la discriminación algorítmica bajo una apariencia de objetividad técnica (Lum & Isaac, 2016, citado en Ramírez Pérez, 2025).

Para mitigar estos riesgos, es imperativo establecer un Protocolo de Gobernanza Algorítmica (PGA) que exija la supervisión y auditoría constante de los modelos de Machine Learning (Ramírez Pérez, 2025). La gobernanza debe garantizar que los resultados algorítmicos sean interpretables y trazables, permitiendo a los operadores judiciales y a la ciudadanía comprender los fundamentos de una decisión predictiva (Sarzaeim et al., 2023, citado en Ramírez Pérez, 2025). Asimismo, es fundamental penalizar el sesgo mediante métricas de desempeño que prioricen la sensibilidad (Recall) en zonas históricamente sub-vigiladas (Ramírez Pérez, 2025).

La hoja de ruta para el periodo 2025-2030 propone formalizar el tránsito hacia un Modelo de Patrullaje Basado en Riesgo (PBR) (Ramírez Pérez, 2025). Este modelo debe utilizar predicciones algorítmicas no para sustituir la intuición policial, sino para optimizar la toma de decisiones en microterritorios, reduciendo el tiempo de respuesta y previniendo la comisión del delito (Ramírez Pérez, 2025). La fase inicial de diseño y pilotaje (2025-2026) debe enfocarse en establecer las bases normativas y reformar los currículos de educación policial para incluir la ciberseguridad (Ramírez Pérez, 2025).

En la fase de expansión (2027-2028), la política criminal debe integrar obligatoriamente variables socioestructurales en los modelos de predicción (Ramírez Pérez, 2025). La analítica de datos no solo debe guiar la respuesta represiva, sino que debe servir para justificar la inversión social en educación, empleo y fortalecimiento comunitario en zonas de alto riesgo criminógeno (Joao & Fernández Romo, 2018, citado en Ramírez Pérez, 2025). Esta visión multinivel busca superar el "modelo penal del castigo" y apostar por una prevención integral que atienda las causas raíces de la delincuencia (Ramírez Pérez, 2025).

La institucionalización de mecanismos como los Centros de Fusión y el Mecanismo de Articulación Interagencial (MAI) es vital para coordinar el flujo de información entre la Policía y la Fiscalía (Londoño-Hurtado et al., 2021, citado en Ramírez Pérez, 2025). El éxito de estos centros en Medellín, que lograron reducir el tiempo de liderazgo de cabecillas

criminales en un 41%, demuestra que la coordinación basada en datos es clave para la persecución penal estructurada (Londoño-Hurtado et al., 2021, citado en Ramírez Pérez, 2025). Hacia el 2030, el Machine Learning debería ser un estándar operativo nacional que trascienda los periodos de gobierno (Ramírez Pérez, 2025).

Desde la perspectiva de la cibercriminología, Colombia debe avanzar en la implementación del Convenio de Budapest para fortalecer la cooperación internacional frente a delitos transfronterizos (Villegas Restrepo & Londoño Rosas, 2024). La naturaleza global del ciberespacio exige tratados de asistencia legal mutua simplificados que agilicen la obtención de evidencia digital respetando los derechos fundamentales (Villegas Restrepo & Londoño Rosas, 2024). Solo a través de una soberanía tecnológica y una infraestructura de datos robusta, el país podrá enfrentar las amenazas emergentes de la cuarta revolución industrial (Villegas Restrepo & Londoño Rosas, 2024).

Finalmente, el compromiso ético debe prevalecer sobre el entusiasmo tecnológico. La justicia penal debe integrar la analítica sin abandonar los principios de racionalidad y dignidad humana (Díaz-Rincón et al., 2024). El reto futuro será consolidar modelos predictivos que no solo sean técnicamente precisos, sino éticamente legítimos y socialmente responsables, garantizando que la innovación tecnológica sirva a la construcción de una paz duradera y una convivencia pacífica en Colombia (Ramírez Pérez, 2025).

En síntesis, la transición hacia una justicia y seguridad mediadas por algoritmos es un cambio de paradigma ineludible (Posada, 2017, citado en Villegas Restrepo & Londoño Rosas, 2024). Si se ejerce bajo un marco de gobernanza transparente, el Estado colombiano podrá reducir los niveles de impunidad y optimizar sus recursos, asegurando que los derechos y libertades fundamentales sean protegidos con la misma firmeza tanto en el mundo físico como en el digital (Villegas Restrepo & Londoño Rosas, 2024).

3.3. Perspectiva comparada entre los sistemas penales de Colombia y México frente al Cibercrimen y la Inteligencia Artificial

En el contexto de la Cuarta Revolución Industrial, tanto Colombia como México enfrentan retos estructurales similares debido a su condición de países en vías de desarrollo, donde la economía depende en gran medida de productos primarios y el acceso a la tecnología no siempre va acompañado de una educación digital robusta (Astaiza Morales & Cuellar Quintero, 2023). Esta realidad socioeconómica genera una dinámica donde la ciudadanía

adquiere dispositivos electrónicos masivamente sin contar con una cultura de ciberseguridad o pedagogía jurídica suficiente para proteger sus derechos fundamentales (Molina, 2010, citado en Astaiza Morales & Cuellar Quintero, 2023). En consecuencia, ambos países se han convertido en terrenos fértiles para conductas criminales virtuales que aprovechan el interés por los nuevos avances económicos y el limitado poder adquisitivo de la población (Astaiza Morales & Cuellar Quintero, 2023).

La falta de recursos económicos en los ciudadanos de naciones como Brasil, México y Colombia impulsa un interés desproporcionado por herramientas tecnológicas que, sin la debida prevención, terminan siendo el vehículo para la comisión de estafas y robos de datos (Astaiza Morales & Cuellar Quintero, 2023). Al compartir estas circunstancias socioeconómicas, la respuesta penal debe trascender la visión local, reconociendo que la delincuencia informática es un fenómeno que afecta a estas instituciones y a las personas naturales por igual, sin discriminación alguna (LE VPN, 2017, citado en Astaiza Morales & Cuellar Quintero, 2023). La vulnerabilidad tecnológica es, por tanto, un rasgo común que exige políticas criminales integrales en la región (Astaiza Morales & Cuellar Quintero, 2023).

Desde una óptica normativa, Colombia ha dado pasos significativos con la Ley mil doscientos setenta y tres de dos mil nueve, logrando una tipificación detallada que protege el bien jurídico de la información y los datos (Astaiza Morales & Cuellar Quintero, 2023). Por su parte, en el ámbito de América del Norte —donde se incluye a México— los modelos de gobernanza y las trayectorias de las políticas de Inteligencia Artificial (IA) muestran una tendencia hacia la regulación de estas tecnologías para optimizar la seguridad nacional (Aguilar, 2024, citado en Díaz-Rincón et al., 2024). No obstante, en ambos países persiste la preocupación por el subjetivismo de los jueces y la posibilidad de que herramientas tecnológicas limiten indebidamente la libertad individual (Rodríguez-Magariños, 2009, citado en Díaz-Rincón et al., 2024).

La eficacia de la persecución penal en Colombia revela una brecha preocupante: mientras el índice de capturas por hurto calificado es del veintidós punto ocho por ciento, para los delitos informáticos es apenas del siete punto uno por ciento (Banca & Economía, 2022, citado en Astaiza Morales & Cuellar Quintero, 2023). Esta baja efectividad es un síntoma de la falta de recursos técnicos y capacitación especializada que también se observa en otros contextos latinoamericanos (Banca & Economía, 2022, citado en Astaiza Morales

& Cuellar Quintero, 2023). En México, por ejemplo, el impacto económico de la violencia interpersonal y criminal proyectado hacia el dos mil treinta subraya la urgencia de adoptar modelos analíticos que permitan optimizar los recursos preventivos del Estado (Cervantes et al., 2023, citado en Ramírez Pérez, 2025).

La implementación de la IA en la justicia colombiana, a través del sistema Prisma, busca reducir el riesgo de reincidencia mediante modelos de aprendizaje supervisado (Fiscalía General de la Nación, 2020, citado en Díaz-Rincón et al., 2024). En México y otros países de la región, el interés por estas herramientas responde a la necesidad de dotar de celeridad a los procesos judiciales y disminuir la percepción de impunidad (Díaz-Rincón et al., 2024). Sin embargo, tanto en el sistema colombiano como en el mexicano, la transición del sistema tradicional al tecnológico-virtual requiere protocolos de asistencia legal mutua que faciliten la obtención de evidencia digital respetando las garantías procesales (Gupta et al., 2023, citado en Díaz-Rincón et al., 2024).

Un desafío compartido es la opacidad algorítmica y el riesgo de que los sistemas de IA funcionen como "cajas negras" (Ramírez Pérez, 2025). Cuando los operadores judiciales en Colombia o México utilizan reportes automáticos para sustentar medidas de aseguramiento, se corre el riesgo de vulnerar el derecho a la defensa si los abogados no pueden controvertir el método matemático subyacente (Pagallo & Quattrocolo, 2018, citado en Díaz-Rincón et al., 2024). Por ello, la gobernanza algorítmica en ambos países debe asegurar que la tecnología sea interpretable y que el criterio ético prevalezca sobre el resultado de la máquina (Khan et al., 2023, citado en Díaz-Rincón et al., 2024).

El fenómeno del "populismo punitivo" también es una constante en las políticas criminales de Colombia y México, donde se privilegia el endurecimiento de penas sobre la prevención basada en evidencia (Gómez, 2020, citado en Ramírez Pérez, 2025). Este modelo penal de castigo ha demostrado ser ineficaz para reducir la criminalidad real, generando en cambio una sobrecarga en los sistemas judiciales y penitenciarios (Gómez, 2020, citado en Ramírez Pérez, 2025). Frente a esto, la criminología computacional surge como una alternativa para racionalizar la toma de decisiones, permitiendo que la policía transite de una reacción intuitiva a una anticipación científica del delito (Sherman, 2013, citado en Ramírez Pérez, 2025).

En México y Colombia, el uso de modelos como Random Forest y XGBoost ha mostrado altos niveles de precisión para identificar hotspots o puntos calientes de criminalidad urbana (Kshatri et al., 2021, citado en Ramírez Pérez, 2025). Estos algoritmos permiten capturar patrones no lineales que los métodos estadísticos tradicionales no logran percibir, facilitando una asignación más equitativa de patrullaje en zonas críticas (Muñoz Jaramillo, 2021, citado en Ramírez Pérez, 2025). No obstante, la viabilidad técnica de estos modelos en ambos países depende de la calidad de los datos georreferenciados, los cuales suelen ser escasos en ciudades intermedias (Gélvez-Ferreira et al., 2022, citado en Ramírez Pérez, 2025).

La ética en el uso de estas tecnologías exige mitigar el sesgo de retroalimentación (Feedback Bias), un riesgo latente tanto en la vigilancia predictiva colombiana como en la mexicana (Lum & Isaac, 2016, citado en Ramírez Pérez, 2025). Si los algoritmos se entrenan con datos históricos que reflejan la estigmatización previa de barrios vulnerables, el sistema simplemente amplificará la vigilancia sobre esas comunidades, perpetuando ciclos de desigualdad (Ramírez Pérez, 2025). Por tanto, la política criminal en ambos estados debe integrar obligatoriamente variables socioestructurales como la pobreza multidimensional para que la analítica fundamente la inversión social (Ardila Chávarro, 2023, citado en Ramírez Pérez, 2025).

La internacionalización de la delincuencia conecta a los delincuentes cibernéticos de Colombia con redes en México y otras partes del mundo, facilitando el intercambio de técnicas de phishing y fraude financiero (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020, citado en Astaiza Morales & Cuellar Quintero, 2023). Esta naturaleza transnacional obliga a ambos países a fortalecer su adhesión al Convenio de Budapest para agilizar la cooperación internacional y la persecución de delincuentes que operan bajo el anonimato de la red (Villegas Restrepo & Londoño Rosas, 2024). El reto es lograr una soberanía tecnológica que permita proteger los datos de los ciudadanos frente a ataques globales (Villegas Restrepo & Londoño Rosas, 2024).

En cuanto a la administración de justicia, la Sentencia T-trescientos veintitrés de dos mil veinticuatro en Colombia marca un precedente relevante para la región al establecer que la IA debe ser solo un instrumento auxiliar para el juez (Díaz-Rincón et al., 2024). En México, el debate jurídico también se encamina a definir los límites de la tecnología para evitar que

los algoritmos sustituyan el pensamiento humano en decisiones que afectan la libertad (Aguilar, 2024, citado en Díaz-Rincón et al., 2024). La imparcialidad debe fundamentarse en los hechos probados y no en supuestos obtenidos de forma irregular a través de la minería de datos (Díaz-Rincón et al., 2024).

La prevención situacional del delito ha sido la estrategia operativa dominante en la vigilancia predictiva de ambos países, pero su enfoque utilitarista a menudo ignora las raíces neoliberales de la motivación delictiva (Joao & Fernández Romo, 2018, citado en Ramírez Pérez, 2025). Tanto en Colombia como en México, la política criminal efectiva debe equilibrar el control tecnológico con estrategias de prevención social y comunitaria (Ramírez Pérez, 2025). El uso de la analítica de datos no debe ser exclusivamente represivo, sino una herramienta para justificar políticas públicas de educación y empleo (Ramírez Pérez, 2025).

La formación policial en ciberseguridad y forense digital es una necesidad urgente compartida. En Colombia, se ha propuesto reformar los currículos educativos de la policía para incluir módulos específicos sobre delitos informáticos (Ávila-Niño & Rincón-Núñez, 2023, citado en Ramírez Pérez, 2025). En México, la sofisticación de los grupos criminales transnacionales exige capacidades similares para enfrentar el lavado de activos y la manipulación informática (Ramírez Pérez, 2025). Sin una policía técnica y científicamente preparada, las leyes contra el cibercrimen seguirán teniendo un impacto ineficaz (Astaiza Morales & Cuellar Quintero, 2023).

Hacia el dos mil treinta, la hoja de ruta para Colombia y México debe incluir la creación de un Data Hub nacional que centralice información delictiva, socioeconómica y de convivencia (Ramírez Pérez, 2025). Este repositorio permitiría superar la limitación de la escasez de datos locales y construir modelos predictivos más robustos y menos sesgados (Ramírez Pérez, 2025). La colaboración interagencial entre la Policía, la Fiscalía y las autoridades locales es el pilar para una persecución penal estructurada, tal como lo han demostrado los Centros de Fusión en ciudades como Medellín (Londoño-Hurtado et al., 2021, citado en Ramírez Pérez, 2025).

La materialidad virtual de los delitos cometidos en el ciberespacio mexicano y colombiano produce daños reales y tangibles que deben ser reparados bajo enfoques de justicia restaurativa (Mesa, 2020, citado en Villegas Restrepo & Londoño Rosas, 2024). Aunque el acto ocurra en un entorno digital, la pérdida de patrimonio y la afectación a la

intimidad tienen consecuencias psicológicas severas que el sistema penal no siempre alcanza a mitigar (Mesa, 2020, citado en Villegas Restrepo & Londoño Rosas, 2024). La legislación debe, por tanto, enfocarse en la protección efectiva de la víctima en el entorno digital (Villegas Restrepo & Londoño Rosas, 2024).

Finalmente, el análisis comparado permite concluir que tanto Colombia como México se encuentran en una encrucijada tecnológica y ética (Ramírez Pérez, 2025). El éxito en la lucha contra la cibercriminalidad dependerá de la capacidad de sus Estados para implementar una gobernanza algorítmica transparente que proteja los valores democráticos (Sarzaeim et al., 2023, citado en Ramírez Pérez, 2025). La IA y el aprendizaje automático ofrecen una oportunidad histórica para mejorar la seguridad ciudadana, siempre que su despliegue esté guiado por el respeto a la dignidad humana y los principios de proporcionalidad (Díaz-Rincón et al., 2024). A diferencia de Colombia en México la regulación específica sobre la IA en el entorno penal es más fragmentada, centrándose en la violencia digital, pero dejando vacíos en la responsabilidad penal por decisiones algorítmicas autónomas.

Conclusiones

En relación con el objetivo general de la investigación, se concluye que la Inteligencia Artificial (IA) ha generado un cambio de paradigma en la configuración de conductas penalmente relevantes, desbordando los marcos normativos tradicionales y exigiendo una revisión profunda de las categorías clásicas de la teoría del delito (Casabona & Martín, 2023, citado en Hector, s.f.). El estudio comparado entre Colombia y México evidencia que ambos Estados enfrentan retos estructurales similares debido a su condición de países en vías de desarrollo, donde la falta de una cultura de ciberseguridad y el interés por los nuevos avances económicos convierten a la ciudadanía en un "blanco fácil" para técnicas de ingeniería social y fraudes automatizados (Astaiza Morales & Cuellar Quintero, 2023). En última instancia, el impacto de la IA en el sistema penal demanda una transición desde modelos punitivos reactivos hacia una gobernanza algorítmica transparente, donde la analítica de datos fundamente no solo la persecución criminal, sino también la inversión social para proteger los derechos fundamentales (Ramírez Pérez, 2025).

Respecto al primer objetivo específico sobre la génesis y el tratamiento jurídico-penal de estas tecnologías, se establece que el origen del ciberdelito en la región está

intrínsecamente ligado a la expansión de la conectividad y la internacionalización de la delincuencia, factores que permiten a los actores locales conectarse con redes globales bajo el anonimato (Ministerio de Tecnologías de la Información y las Comunicaciones, 2020, citado en Astaiza Morales & Cuellar Quintero, 2023). En Colombia, el hito normativo fue la Ley mil doscientos setenta y tres de dos mil nueve, la cual tipificó conductas como la interceptación de datos y el daño informático; sin embargo, el tratamiento de la IA sigue siendo incipiente tanto en el ordenamiento colombiano como en el mexicano (Astaiza Morales & Cuellar Quintero, 2023; Quiñones et al, 2025, citado en Hector, s.f.). La efectividad de estos marcos legales se ve limitada por una asimetría tecnológica donde las técnicas delictivas evolucionan a una velocidad superior a la capacidad de respuesta institucional, lo que subraya la necesidad de fortalecer tratados internacionales como el Convenio de Budapest (Clough, 2010, citado en Villegas Restrepo & Londoño Rosas, 2024).

Frente al segundo objetivo específico sobre los problemas dogmáticos y la funcionalidad tecnológica, la investigación determina que la IA plantea tensiones críticas sobre la noción de acción y la imputación objetiva, debido a que la opacidad algorítmica o "caja negra" dificulta establecer el nexo causal entre el programador y el resultado lesivo (Ojeda, 2026, citado en Hector, s.f.; Gallegos, 2022, citado en Hector, s.f.). En la práctica judicial, herramientas como el sistema Prisma en Colombia demuestran que, si bien el Machine Learning aporta celeridad y ayuda a descongestionar despachos, su uso genera riesgos de subjetivismo y sesgos algorítmicos que pueden vulnerar la presunción de inocencia (Díaz-Rincón et al., 2024). La viabilidad técnica de estos modelos alcanza precisiones de hasta el ochenta y seis por ciento en entornos urbanos complejos, pero su eficacia decae en ciudades intermedias por el limitado acervo de información georreferenciada, lo que exige una estandarización de los datos a nivel nacional (Muñoz Jaramillo, 2021, citado en Ramírez Pérez, 2025; Gélvez-Ferreira et al., 2022, citado en Ramírez Pérez, 2025).

Finalmente, en cuanto al tercer objetivo específico sobre las respuestas de política criminal y los lineamientos futuros, se concluye que es imperativo superar el "populismo punitivo" y el modelo penal del castigo que ha generado niveles de impunidad cercanos al cincuenta y ocho por ciento (Gómez, 2020, citado en Ramírez Pérez, 2025). Las políticas proyectadas para el periodo dos mil veinticinco-dos mil treinta deben formalizar el tránsito hacia un Servicio de Policía Basado en la Evidencia (EBP), integrando obligatoriamente

variables socioestructurales como la pobreza multidimensional en los modelos predictivos (Ramírez Pérez, 2025; Ardila Chávarro, 2023, citado en Ramírez Pérez, 2025). La creación de un Protocolo de Gobernanza Algorítmica (PGA) y el fortalecimiento de la cooperación regional entre Colombia y México permitirán mitigar el sesgo de retroalimentación (Feedback Bias), garantizando que la innovación tecnológica sirva a la justicia y a la paz duradera sin abandonar los principios de racionalidad y dignidad humana (Ramírez Pérez, 2025; Díaz-Rincón et al., 2024).

Referencias

Aguilar, J. M. (2024). Trayectoria y modelo de gobernanza de las políticas de inteligencia artificial (IA) de los países de América del Norte. Justicia, 29(45), 1-19. https://doi.org/10.17081/just.29.45.7162

Ardila Chávarro, M. C. (2023). Crimen y Factores Económicos en Medellín: Un Estudio de Predicción con Machine Learning (Tesis de Maestría). Universidad del Rosario

Astaiza Morales, P. A., & Cuellar Quintero, V. (2023). Análisis dogmático de los delitos informáticos o ciberdelitos en Colombia (Monografía de grado). Universidad Libre Seccional Cali

Ávila-Niño, F. Y., & Rincón-Núñez, P. M. (2023). Inclusión de la formación en prevención y atención de delitos informáticos en la educación policial. Revista Educación, 47(2)

Baker, D. J., & Robinson, P. H. (Eds.). (2021). Artificial Intelligence and the Law. Cybercrime and Criminal Liability. Routledge

Banca & Economía. (2022). Eficiencia de la política pública de delitos informáticos. Asobancaria

Casabona, C. M. R., & Martín, M. Á. R. (2023). Derecho penal, ciberseguridad, ciberdelitos e inteligencia artificial. Editorial Comares

Clough, J. (2010). Principles of Cybercrime. Cambridge University Press

Díaz-Rincón, S. V., Enamorado-Estrada, J. A., & Bolaño-Retamozo, N. M. (2024). La inteligencia artificial en la solicitud e imposición de la medida de aseguramiento en el derecho penal de Colombia. Revista Jurídicas, 21(2), 199-220. https://doi.org/10.17151/jurid.2024.21.2.11

Dunne, R. (2009). Computers and the law. An Introduction to Basic Legal Principles and Their Application in Cyberspace. Cambridge University Press

Gélvez-Ferreira, J. D., Helfer, P. M., Rodríguez, M. P. N., & Ruiz, C. A. R. (2021). Predicción del delito en Colombia: experiencia en ciudades intermedias. Dirección de Estudios Económicos

Gómez, O. (2020). Efectividad de la política criminal colombiana hacia la prevención del delito. Revista Criminalidad, 62(3)

Hernández Chinome, V., & López-Zamora, S. A. (2025). IA: Hacia la deshumanización del derecho. *Revista Principia Iuris*, *22*(46), 181-191.

Holt, T. J., & Bossler, A. M. (Eds.). (2020). The Palgrave Handbook of International Cybercrime and Cyberdeviance. Palgrave Macmillan

Jahankhani, H. (2018). Cyber Criminology. Springer

Jaishankar, K. (2008). Space Transition Theory of Cyber Crimes. En F. Schmallager & M. Pittaro (Eds.), Crimes of the Internet (pp. 283-301). Prentice Hall

Jaishankar, K. (Ed.). (2011). Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. CRC Press

Joao, F. L., & Fernández Romo, R. M. (2018). La prevención del delito a través de prácticas situacionales. IUSTA, (16)

Khan, A. A., Akbar, M. A., Fahmideh, M., Liang, P., Waseem, M., Ahmad, A., & Abrahamsson, P. (2023). AI ethics: an empirical study on the views of practitioners and lawmakers. IEEE Transactions on Computational Social Systems. https://doi.org/10.1109/TCSS.2023.3251729

LE VPN. (2017). Historia del ciberdelito

Lorduy, J. (2022). Más de 29.000 ciberdelitos se han denunciado en 2022. Portafolio

Lum, K., & Isaac, W. (2016). To predict and serve? Significance, 13(5), 14–19

Mesa, M. (2020). La Materialidad Virtual y sus Implicaciones Legales. Revista de Derecho Informático, 27(1), 50-68

Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). (2020). Estrategia Nacional de Ciberseguridad. Colombia

Molina, F. (2010). Pedagogía jurídica y derechos fundamentales

Muñoz Jaramillo, V. D. (2021). Evaluación de Modelos de Machine Learning para la Predicción de Crímenes en la Ciudad de Medellín (Tesis de Maestría). Universidad Nacional de Colombia

Owen, T., & Savage, J. (2015). Criminología y entorno digital. Palgrave Macmillan

Pagallo, U., & Quattrocolo, S. (2018). The impact of AI on criminal law, and its twofold procedures. En W. Barfield & U. Pagallo (Eds.), Research Handbook on the Law of Artificial Intelligence. Edward Elgar Publishing

Pérez, Rodríguez, Flórez & Martínez. (2010). Investigación sobre delitos informáticos en Colombia

Ramírez Camacho, A. M., Mesa Velandia, L. D., & Ramírez Ramírez, N. S. (2020). Los derechos fundamentales de las víctimas de los ciberdelitos en Colombia. Institución Universitaria Politécnico Grancolombiano

Ramírez Pérez, E. (2025). Seguridad nacional en Colombia: un enfoque analítico para la prevención del delito (Monografía de especialización). Universidad Nacional Abierta y a Distancia UNAD

Rodríguez-Magariños, F. (2009). La paulatina erradicación de la prisión preventiva: Un análisis progresivo bajo las potencialidades de las nuevas tecnologías. Boletín del Ministerio de la Presidencia, Justicia y Relaciones con las Cortes, 63(2078), 227-254

Sherman, L. W. (2013). Evidence-Based Policing. Police Foundation

Suler, J. (2004). The Online Disinhibition Effect. CyberPsychology & Behavior, 7(3), 321-326

Villegas Restrepo, J. A., & Londoño Rosas, W. A. (2024). Cibercriminología y política criminal: fundamentos para una implementación legislativa en Colombia (Trabajo de grado de maestría). Universidad Externado de Colombia