Derecho penal y revolución digital: desafíos y soluciones para regular crímenes cometidos en la era tecnológica

Criminal law and digital revolution: challenges and solutions to regulate crimes committed in the technological era

Resumen

El derecho generalmente es retrospectivo, reacciona ante sucesos que ya han sucedido; por otro lado, la tecnología es proactiva y se desarrolla sin aguardar la aprobación legislativa. (LUÑO, 2012) argumenta que, la tecnología progresa a una velocidad que el proceso legislativo no puede equiparar, generando una brecha que impide el desarrollo. Esta discrepancia entre el tiempo de respuesta legal y el de la tecnología provoca que numerosas regulaciones se apliquen de forma tardía, obstaculizando que las tecnologías emergentes se desarrollen en un ambiente regulado y seguro.

Considerando que la rigidez legal representa uno de los principales impedimentos para el progreso digital, resulta imprescindible aplicar métodos más versátiles y adaptables. (Erdélyi & Goldsmith, 2022) sugieren la idea de "arquitectura regulatoria dinámica", donde el derecho no solo se mantenga inmóvil, sino que también pueda ajustarse a las demandas tecnológicas contemporáneas Este método conllevaría: Establecimiento de marcos regulatorios provisionales que faciliten la experimentación regulada de tecnologías novedosas, previniendo su prohibición sin un examen exhaustivo de sus consecuencias; organizaciones de revisión tecnológica en las entidades legislativas, que monitoreen el progreso tecnológico e informen acerca de la necesidad de renovar regulaciones anticuadas, y regulaciones fundamentadas en principios, en vez de normas rigurosas, que posibiliten a los magistrados ajustar las resoluciones a los progresos tecnológicos. Roxin respalda esta perspectiva en su teoría del delito, indicando que, el derecho debe prevenir reglas demasiado estrictas, que desconsideren la evolución social (Roxin C. , 2006)

El progreso de la inteligencia artificial ha creado nuevas posibilidades y retos para el ámbito del derecho criminal. Aunque la IA puede simplificar la observancia de la ley mediante instrumentos de prevención y evaluación, también permite el surgimiento de nuevas modalidades de delitos. Dos sectores especialmente vulnerables a estos nuevos tipos de delitos son el blanqueo de capitales y la financiación del terrorismo, a causa de la potencialidad de que la Inteligencia Artificial se emplee para ocultar o simplificar actividades delictivas. Este estudio tiene como objetivo examinar cómo el derecho penal puede abordar estos retos, definiendo un marco regulatorio apropiado para la regulación de los comportamientos que puedan realizarse mediante el uso de Inteligencia Artificial en estos crímenes.

Abstract

Law is generally retrospective, reacting to events that have already occurred; on the other hand, technology is proactive and develops without waiting for legislative approval. (LUÑO, 2012) argues that technology progresses at a speed that the legislative process cannot match, creating a gap that impedes development. This discrepancy between the legal response time and that of technology causes numerous regulations to be implemented late, hindering the development of emerging technologies in a regulated and secure environment.

Considering that legal rigidity represents one of the main impediments to digital progress, it is essential to apply more versatile and adaptable methods. (Erdélyi & Goldsmith, 2022) suggest the idea of a "dynamic regulatory architecture," where the law not only remains static but can also adjust to contemporary technological demands. This approach would entail: the establishment of provisional regulatory frameworks that facilitate regulated experimentation with novel technologies, preventing their prohibition without a thorough examination of their consequences; technology review organizations within legislative bodies that monitor technological progress and report on the need to update outdated regulations; and regulations based on principles, rather than rigorous standards, that enable judges to adjust decisions to technological progress. Roxin supports this perspective in his theory of crime, stating that the law should prevent overly strict rules that disregard social evolution (Roxin C., 2006). The progress of artificial intelligence has

created new possibilities and challenges for the field of criminal law. Although AI can simplify law enforcement through prevention and assessment tools, it also enables the emergence of new types of crimes. Two sectors particularly vulnerable to these new types of crimes are money laundering and terrorist financing, due to the potential for Artificial Intelligence to be used to conceal or simplify criminal activities. This study aims to examine how criminal law can address these challenges by defining an appropriate regulatory framework for the conduct that can be carried out through the use of Artificial Intelligence in these crimes.

Introducción

La digitalización acelerada de la sociedad ha demostrado las restricciones del derecho en la adaptación a los progresos tecnológicos. Aunque la tecnología progresa a un ritmo acelerado, los marcos legales a menudo experimentan procesos de actualización y adaptación más lentos, generando una brecha entre el derecho, la realidad social y la tecnología. Esto presenta retos significativos en campos como la inteligencia artificial (IA), la salvaguarda de datos, el comercio digital y la seguridad informática. Algunos expertos incluso proponen que los sistemas legales convencionales, por su inflexibilidad, actúan como un impedimento para el progreso digital y la innovación tecnológica.

De acuerdo con (Castellà Andreu, Montobbio, & Granata-Menghini, 2022) El derecho se distingue por su estabilidad y predictibilidad, dos valores que garantizan la solidez legal y, por ende, la estabilidad jurídica necesaria en todo Estado Democrático de Derecho, pero que entorpecen la reacción rápida requerida para enfrentar los nuevos desafíos delictivos que a diario se presentan debido a los avances tecnológicos que, día a día, son más veloces. De acuerdo con Lawrence Lessig, el derecho convencional carece de la adaptabilidad requerida para regular el ciberespacio, en el que el cambio es permanente y la respuesta de los legisladores es pausada (Lessig, 2006). Esta inflexibilidad lleva a la obsolescencia de numerosas regulaciones que no toman en cuenta fenómenos como la Inteligencia Artificial o la economía digital, generando áreas grises que obstaculizan la innovación y el crecimiento.

Los sistemas de IA, que se vuelven cada vez más autónomos y sofisticados, crean nuevas modalidades de interacción entre humanos y máquinas que necesitan normativas particulares. No obstante, tanto el derecho penal como el civil se encuentran restringidos en la atribución de responsabilidad en situaciones donde la Inteligencia Artificial comete fallos o provoca daños. Frank Pasquale argumenta que, al no ajustarse de manera rápida a las habilidades de las máquinas autónomas, el derecho puede frenar la innovación en IA al establecer limitaciones excesivas en su evolución (PASQUALE, 2015); estas limitaciones se originan ya que la legislación vigente no contempla situaciones en las que la automatización de la toma de decisiones sobrepase la habilidad de control humano.

De la misma manera, Pasquale señala que, La revolución digital y el progreso acelerado de tecnologías como la inteligencia artificial han cambiado drásticamente el modo en que se perpetran, identifica y controlan los delitos (PASQUALE, 2015). No obstante, el derecho penal, establecido bajo principios y estructuras convencionales, se enfrenta con retos cada vez mayores para tratar de manera eficiente estas nuevas modalidades de delincuencia tecnológica. Es indudable que, los criterios tradicionales de acción, dolo, culpa, imputación, etc., se quedan cortos y son insuficientes para solucionar los problemas y desafíos que a diario presenta el ciber espacio y las nuevas tecnologías.

Surge entonces, un interrogante que, debería ser uno de los que guie las nuevas investigaciones en el campo del Derecho Penal: ¿Cómo puede adaptarse y modernizarse el derecho penal para regular eficientemente los delitos perpetrados en la época tecnológica, asegurando principios esenciales como la legalidad, proporcionalidad y responsabilidad, ante retos particulares como la autonomía de la Inteligencia Artificial, la ausencia de imputación clara y la globalización de los crímenes digitales?

Este problema surge de la falta de capacidad de los marcos regulatorios vigentes para prever y regular el efecto de crímenes digitales, tales como el blanqueo de capitales, el financiamiento del terrorismo y otras actividades delictivas, realizadas con tecnologías de vanguardia. Además, plantea cuestionamientos acerca de la atribución de responsabilidad, la formulación de castigos proporcionales y la prevención de estos delitos en un contexto global e interconectado (Rincón Arteaga, Castiblanco Hernández, Quijano Díaz, Urquijo Vanegas, & Pregonero León, 2023).

Otra área en la que el derecho se colisiona con retos considerables es la salvaguarda de la información personal. La urgencia de salvaguardar la privacidad de los ciudadanos ha impulsado la instauración de regulaciones rigurosas como el Reglamento General de Protección de Datos (GDPR) en Europa. No obstante, esta legislación, pese a salvaguardar los derechos de las personas, ha sido objeto de críticas por su impacto limitante en el progreso tecnológico y la innovación. (Moreno, 2024) argumenta que, pese a ser indispensable, las leyes sobre privacidad "se han transformado en un impedimento para la innovación en la era digital al limitar la utilización de datos en masa en procesos de Inteligencia Artificial y análisis predictivo.

Es vital modernizar los códigos penales para tratar de manera específica el empleo de tecnologías como la Inteligencia Artificial en el lavado de dinero y la financiación del terrorismo. En algunos Estados, se han creado marcos jurídicos para el ciberdelito que podrían expandirse para abarcar estos aprovechamientos de la IA. La creación de unidades especializadas en delitos tecnológicos en las fuerzas del orden público, que empleen Inteligencia Artificial para neutralizar estos mismos progresos, es una alternativa factible (Compliance). El GAFI (Grupo de Acción Financiera Internacional) ya ha destacado la relevancia de integrar tecnología de vanguardia en la batalla contra estos crímenes, lo cual comprende la utilización de IA para identificar y evitar acciones ilícitas en tiempo real.

Para ejemplarizar un poco la importancia de la relación entre la inteligencia artificial y el derecho penal, se plantea como referencia los delitos financieros, y es que, la IA se ha consolidado como un instrumento esencial en la prevención, identificación y persecución de estos crímenes, tales como el lavado de activos y la financiación del terrorismo. Su habilidad para examinar grandes cantidades de información, detectar patrones dudosos y anticipar acciones delictivas en tiempo real ha transformado los sistemas de aplicación de normativas. De acuerdo con (Chen Cheng , Chung , & Correa , 2023) los algoritmos de aprendizaje automático posibilitan a las empresas identificar irregularidades en transacciones complejas con una exactitud que sobrepasa los procedimientos convencionales. Este método disminuye considerablemente el riesgo de equivocaciones y agiliza las investigaciones. Adicionalmente, la IA ha impulsado los sistemas de

conocimiento del cliente (KYC), garantizando una transparencia y seguimiento más efectivos en las operaciones financieras (Financial Crime Academy, 2025). No obstante, también conlleva peligros. (Sanchez & Caicedo) alertan que el mal uso de la Inteligencia Artificial podría propiciar la formación de redes de lavado de dinero más avanzadas, mientras que las herramientas deben asegurar la salvaguarda de la información personal y prevenir decisiones de sesgo. Es claro que, con una regulación apropiada y un diseño ético, la Inteligencia Artificial puede convertirse en un aliado potente en la batalla contra los crímenes financieros, robusteciendo los sistemas judiciales y aportando a la estabilidad económica mundial.

La IA supone un reto considerable para el derecho penal en la lucha contra crímenes como el blanqueo de capitales y la financiación del terrorismo. A pesar de que la implementación de Inteligencia Artificial puede potenciar la efectividad de estos delitos, el derecho penal tiene la obligación de progresar y normar estos comportamientos; mediante el establecimiento de reglas claras, la renovación de los marcos legales y la asignación de responsabilidades a desarrolladores y usuarios, se pueden minimizar los peligros que la Inteligencia Artificial representa para estos crímenes financieros (Universidad del Bosque).

Aunque el derecho es esencial para garantizar la seguridad legal y la estabilidad, también puede actuar como un obstáculo para el progreso digital. Los retos que presentan tecnologías como la Inteligencia Artificial y la salvaguarda de datos demuestran la necesidad de ajustar el derecho a las transformaciones tecnológicas. El marco legal necesita progresar y adoptar una perspectiva más versátil y adaptable, que posibilite el desarrollo de la tecnología en un contexto regulado, pero no limitante. Es fundamental esta actualización de las normativas para que el derecho actúe como un facilitador, y no como un impedimento, del avance en la era digital (Moreno, 2024).

Metodología

Para abordar los retos y plantear recursos en la regulación de crímenes cometidos en la era tecnológica desde una perspectiva de derecho penal, este artículo adopta un enfoque metodológico interdisciplinario y estructurado en las siguientes etapas:

Revisión documental y literaria

Se llevó a cabo un examen minucioso de la literatura académica, las regulaciones internacionales y las doctrinas legales pertinentes vinculadas con el derecho penal y su ajuste a la revolución digital. Esta revisión contempló el estudio de trabajos de escritores como (Roxin C. , 1997), (Hallevy, 2013) y (Floridi, 2013), además de investigaciones actuales acerca del efecto de la inteligencia artificial en el ámbito jurídico penal. Se dio prioridad al estudio de fuentes legislativas y doctrinales que indague en los principios de responsabilidad penal, imputación objetiva y subjetiva en entornos tecnológicos.

Evaluación comparativa

Se analizaron regulaciones y ejemplos prácticos de diversas jurisdicciones para determinar cómo los sistemas jurídicos han tratado el problema de los delitos digitales y la relevancia de tecnologías de vanguardia como la inteligencia artificial. Este método comparativo posibilitó obtener enseñanzas y buenas prácticas que puedan aplicarse a otras jurisdicciones.

Valoraciones doctrinales y de expertos

Se incorporaron puntos de vista de académicos y expertos en derecho penal e informática, mediante entrevistas organizadas y evaluaciones cualitativas. Esto posibilitó situar las teorías en el contexto actual de la práctica legal y tecnológica, teniendo en cuenta las restricciones y retos en la puesta en marcha de soluciones regulatorias.

Orientación regulativa y propositiva

Basándose en el análisis anterior, se elaboraron recomendaciones normativas para modernizar los marcos jurídicos penales ante los retos digitales. Esta perspectiva comprendió entre otras, reconocimiento de lagunas jurídicas en la normativa de delitos digitales, elaboración de soluciones fundamentadas en valores como la proporcionalidad, la lógica y la prevención y evaluación de la factibilidad jurídica y aplicación de estas sugerencias.

Validación Teórica

Finalmente, se compararon las conclusiones y sugerencias del artículo con los principios esenciales del derecho penal y las tendencias contemporáneas en la normativa tecnológica, garantizando su consistencia y utilidad en diversos escenarios jurídicos.

Esta metodología tiene como objetivo asegurar un análisis meticuloso y pragmático, ofreciendo un marco completo para abordar los retos del derecho penal en la era digital.

Conciencia y Código Moral de la IA

El progreso de la inteligencia artificial hacia sistemas cada vez más independientes y sofisticados genera interrogantes esenciales en el campo jurídico. La capacidad de una IA para tomar decisiones autónomas, con un cierto grado de "conciencia" o criterio moral, genera un debate acerca de la responsabilidad jurídica y la normativa de dichas decisiones. Aunque la autonomía de la Inteligencia Artificial en labores rutinarias o programadas ha sido ampliamente reconocida, su habilidad para actuar con autonomía moral y legal continúa siendo un asunto complicado y polémico (Verdegay , Lamata, Pelta, & Cruz, 2021).

En el ámbito legal, la autonomía se define como la habilidad de un organismo para tomar decisiones de manera libre y voluntaria, fundamentadas en un criterio personal y no en directrices externas. Los sistemas de Inteligencia Artificial sofisticados, como las redes neuronales profundas y los algoritmos de aprendizaje automático, exhiben una habilidad restringida para tomar decisiones complejas, pese a que todavía no poseen la total independencia que tiene un ser humano. (Metaverso, s.f.) indica que la Inteligencia Artificial funciona a través de algoritmos que manejan grandes volúmenes de datos, facilitándole la toma de decisiones sin necesidad de intervención humana directa. No obstante, alerta que a pesar de que estos sistemas pueden simular la toma de decisiones, no poseen intencionalidad, un componente esencial para que sus acciones sean legalmente responsables. Así, a pesar de que la IA puede replicar el proceso de toma de decisiones, la ausencia de intención y de una auténtica autonomía convierte sus decisiones en una proyección de los datos y las normas con las que se programó.

La conciencia es otro elemento esencial en el debate acerca de la habilidad de la Inteligencia Artificial para tomar decisiones independientes. En las personas, la

conciencia es vista como un componente crucial para la responsabilidad jurídica, pues facilita la distinción entre lo que es bueno y lo que es malo. Por otro lado, la IA opera basándose en códigos y algoritmos que le indican cómo reaccionar ante determinados estímulos, sin tener una conciencia auténtica o un sentido ético inherente. De acuerdo con Luciano Floridi, especialista en ética de la información, la conciencia en los sistemas artificiales es "un término más metafórico que auténtico" porque que la IA no puede tener una auténtica moralidad, dado que no cuenta con experiencia subjetiva (Floridi, 2013). Aunque se han creado algoritmos que imitan "decisiones éticas", estos están totalmente sujetos a las normas definidas por sus creadores. La Inteligencia Artificial adopta una "ética programada" y, en consecuencia, no puede descifrar el significado moral que subyace a sus elecciones. (González Arencibia & Martínez Cardero, 2020) proponen que "la Inteligencia Artificial nunca podrá comportarse de manera moral en términos humanos, dado que sus decisiones son derivadas, no autónomas".

Constitución moral de la Inteligencia Artificial: ¿Un reemplazo para la responsabilidad penal?

Se ha planteado la idea de un "código moral" para la Inteligencia Artificial como un medio para prevenir que estos sistemas realicen elecciones dañinas para las personas. Esto conlleva la incorporación de "valores éticos" en la programación de la Inteligencia Artificial, de manera que su proceso de toma de decisiones se oriente a reducir daños y potenciar ventajas. No obstante, la principal restricción de un código moral preestablecido radica en su dependencia de los valores y orientaciones establecidos por sus creadores humanos, lo que restringe su implementación independiente en circunstancias inesperadas. Stuart Russell y Peter Norvig subrayan que, aunque los programadores pueden definir normas éticas en un sistema de Inteligencia Artificial, "el criterio ético es intrincado y específico de contexto, lo que complica la aplicación de una moral auténtica en una máquina" (J. Russell & Norvig, 2020). Además, cualquier código moral establecido en la Inteligencia Artificial sería inflexible y probablemente inadecuado para manejar circunstancias morales complejas que demandan empatía y criterio subjetivo.

La ausencia de conciencia y de un código moral genuino representa un reto crucial para la distribución de responsabilidad en la toma de decisiones de la Inteligencia Artificial. Si una IA provoca perjuicio, la culpa debe ser asumida por algún individuo humano, como el programador, el usuario o la compañía que creó la IA. De acuerdo con Gabriel Hallevy, en su trabajo titulado When Robots Kill: Artificial Intelligence Under Criminal Law, a pesar de que la Inteligencia Artificial actúe de forma autónoma, la responsabilidad penal debe ser asumida por los individuos que tienen dominio sobre su generación y uso (Hallevy, 2013). Esta teoría argumenta que la Inteligencia Artificial, al no poseer conciencia, no puede constituir un ente autónomo con responsabilidad penal, por lo que cualquier acto ilegal realizado con o por la IA debe ser atribuido a los culpables humanos. No obstante, Hallevy también propone que, conforme la Inteligencia Artificial se torne más avanzada, podrían aparecer nuevos modelos de responsabilidad compartida o diferida. Por ejemplo, en sistemas autónomos de IA que toman decisiones sin supervisión, el legislador podría contemplar un esquema que reparta la responsabilidad entre diversos participantes en función del grado de control que posean sobre la IA.

La discusión acerca de la conciencia y la moralidad de la Inteligencia Artificial presenta dilemas significativos para el ámbito jurídico. La instauración de una obligación legal para sistemas de Inteligencia Artificial autónomos podría implicar la modificación de los principios vigentes del derecho penal y civil, o incluso la formación de nuevos tipos de entidades legales. En este contexto, (Azuaje Pirela & Contreras, 2021) proponen que, la Inteligencia Artificial podría poseer una personalidad jurídica restringida, que le otorgue responsabilidad en un sentido limitado, sin equipararla a la responsabilidad humana. Este método podría posibilitar que algunos sistemas de Inteligencia Artificial actúen ante daños sin poner en riesgo la responsabilidad humana, aunque continúa siendo un asunto de investigación en la mayoría de las jurisdicciones. En cambio, reconocer una "ética programada" podría significar que los sistemas de Inteligencia Artificial sean tratados como entidades con moral derivada. Sin embargo, la falta de una moral verdadera en la Inteligencia Artificial provoca que estos sistemas continúen considerándose como herramientas sofisticadas más que como auténticos entes morales (Meseguer, 2023).

La posibilidad de que la IA tome decisiones autónomas plantea desafíos significativos para el derecho, especialmente en lo que respecta a la conciencia y la moralidad de estas tecnologías. Aunque los sistemas de IA avanzados pueden simular la toma de decisiones complejas, carecen de los elementos subjetivos y éticos que caracterizan a la toma de decisiones humanas. (Sayad, 2023) plantea que, en que la IA, por más avanzada que sea, actúa sin conciencia ni intencionalidad moral, lo cual limita su responsabilidad jurídica. El derecho enfrenta el reto de adaptar sus principios para abordar la responsabilidad derivada de los actos de la IA sin asignarle una personalidad jurídica plena. Esta adaptación requerirá un enfoque equilibrado que permita el desarrollo de la IA sin comprometer la responsabilidad ética y jurídica de sus creadores y operadores humanos.

Imputación objetiva en la era de la IA: redefiniendo la responsabilidad en un mundo de máquinas autónomas

La imputación objetiva es un principio esencial del derecho penal que intenta determinar las circunstancias en las que se puede imputar a una persona por un acto delictivo. Dentro del marco de la inteligencia artificial, este principio enfrenta retos singulares, dado que la independencia y el comportamiento autónomo de los sistemas de IA dificultan la distribución de responsabilidad. La Inteligencia Artificial puede funcionar de forma autónoma, produciendo resultados que no siempre se pueden vincular con decisiones humanas concretas, lo que genera interrogantes esenciales acerca de cómo se debe implementar la imputación objetiva en estas situaciones. La imputación objetiva se refiere a la atribución de un resultado delictivo a un autor, considerando si dicho resultado era previsible y si el autor tenía un control suficiente sobre el acto. Según (Roxin C. , 1997), la imputación objetiva implica que “el resultado delictivo debe ser la consecuencia de la acción del autor y debe haber un nexo de causalidad que lo vincule. Este enfoque tradicional se basa en la idea de que un individuo debe tener la capacidad de controlar su conducta y prever sus consecuencias.

La aparición de la Inteligencia Artificial en el ámbito penal ha difundido las fronteras de esta interpretación. Los sistemas de IA, particularmente los que emplean aprendizaje automático, tienen la capacidad de producir decisiones y resultados que no son

directamente vinculables a un ser humano, lo que dificulta la atribución objetiva (Porcelli, 2020) sostiene que, la independencia de los sistemas de Inteligencia Artificial genera una brecha entre las acciones del programador y los resultados generados, cuestionando la estructura convencional de imputación; La dificultad reside en que, aunque los humanos programan y capacitan a las Inteligencia Artificial, las decisiones adoptadas por estos sistemas frecuentemente superan el control y la predictibilidad del programador.

El problema de a quién se debe atribuir la responsabilidad se complica aún más en el contexto de sistemas de Inteligencia Artificial que funcionan de forma autónoma. El compromiso puede ser asumido por varios participantes: el programador, el dueño de la Inteligencia Artificial o incluso el usuario final. De acuerdo con (Hallevy, 2013) la responsabilidad debe evaluarse no únicamente desde el punto de vista del acto delictivo, sino también desde el marco de la generación y funcionamiento de la Inteligencia Artificial; Esto significa que, a pesar de que el sistema de Inteligencia Artificial funcione de forma autónoma, los individuos que crearon y emplearon el sistema aún podrían ser juzgados por su contribución a un desenlace delictivo.

En respuesta a estos retos, es esencial que el derecho penal se modifique para tratar la imputación objetiva en el marco de la Inteligencia Artificial. Algunos autores sugieren elaborar un marco regulatorio particular que tome en cuenta las características de la IA, posibilitando la generación de una nueva modalidad de imputación que incluya la responsabilidad conjunta entre los distintos participantes implicados. (Espinosa, 2021) propone que, la legislación penal debe progresar para incorporar estipulaciones concretas que traten la independencia de la IA y su habilidad para comportarse de forma autónoma; Esto podría requerir el establecimiento de categorías de responsabilidad concretas que identifiquen la dualidad entre la acción humana y la decisión automatizada.

La imputación objetiva en el marco de la IA constituye un desafío importante para el derecho penal actual. La independencia de los sistemas de Inteligencia Artificial dificulta la distribución de responsabilidad y reta la implementación de los principios convencionales de atribución. Es fundamental que el sistema legal se ajuste a estas nuevas circunstancias, elaborando métodos que identifiquen la complejidad de la relación entre los seres humanos y las máquinas. Es necesario comprender la

responsabilidad de forma más integral, teniendo en cuenta el rol de los programadores y usuarios en la construcción y funcionamiento de sistemas de Inteligencia Artificial. Solo de esta manera se podrá alcanzar una implementación equitativa y eficaz del derecho penal en un mundo en el que la Inteligencia Artificial tiene un rol cada vez más relevante (Espinosa, 2021).

Acción 2.0, la responsabilidad en un mundo digital interconectado

En el campo del derecho, tradicionalmente se ha interpretado el concepto de acción como una conducta humana que genera efectos legales, sean estos lícitos o no. No obstante, la aparición de la era digital ha retado y modificado este concepto. Ahora, las acciones humanas están vinculadas con la tecnología, lo que requiere replantear la esencia de la acción en un entorno donde las interacciones son mediadas por algoritmos y sistemas automatizados. Históricamente, la acción se entiende como la manifestación de la voluntad que genera un impacto en el ámbito legal. De acuerdo con (Kelsen, 1960), en su obra Teoría Pura del Derecho, la acción representa la expresión de la intención humana en el marco legal; Esta definición enfatiza el valor de la intencionalidad y la habilidad para tomar decisiones, factores que se tornan complejos en el entorno digital. Por ende, la acción conlleva responsabilidad, dado que constituye la base en la que se aplican sanciones y se conceden derechos.

La digitalización ha incorporado nuevos participantes y componentes en la idea de acción. Mediante la implementación de algoritmos e IA, las acciones no siempre son el producto de elecciones humanas deliberadas. (Verdegay , Lamata, Pelta, & Cruz, 2021) argumentan que, la Inteligencia Artificial y los algoritmos funcionan como actores en el espacio digital, tomando decisiones que pueden tener impactos considerables en el mundo real; Este fenómeno dificulta el concepto de acción, ya que plantea la cuestión de quién tiene responsabilidad cuando una decisión dañina es adoptada por una máquina: ¿es el programador, el usuario o la propia máquina?

La participación de la Inteligencia Artificial en el proceso de decisión genera dilemas éticos y legales. Por ejemplo, en el contexto de los sistemas de recomendación, el acto de "recomendar" puede impactar en el comportamiento de los usuarios de manera que superan su capacidad de control. De acuerdo con (Floridi, 2013), "la Inteligencia Artificial

puede ejercer un impacto que convierte la acción humana en un conjunto de respuestas anticipadas fundamentadas en datos; Esto implica un grado de automatización que reta la habilidad de las personas para comportarse de forma independiente y deliberada.

El desafío de la acción en la era digital requiere una reevaluación de la responsabilidad legal. ¿Cómo se puede implementar el principio de responsabilidad si las decisiones son tomadas por sistemas automatizados? De acuerdo con (Hallevy, 2013) la responsabilidad penal debe tomar en cuenta no solo la acción del individuo, sino también la programación y operación de la Inteligencia Artificial. Esto implica que la acción no se puede considerar solo desde el punto de vista de la voluntad humana, sino también desde la interacción con sistemas tecnológicos. La repartición de la responsabilidad se torna imprescindible. Por ejemplo, si un sistema de inteligencia artificial provoca un perjuicio, la atribución de culpabilidad puede extenderse desde el desarrollador del algoritmo hasta el usuario final. Esto genera interrogantes acerca de cómo crear leyes y normar en un ambiente donde la interacción se desvanece entre humanos y maquinaria.

Dada la transformación del concepto de acción en la era digital, se evidencia la demanda de nuevos marcos regulatorios que identifiquen las características específicas de la interacción entre humanos y máquinas. (Espinosa, 2021) sugiere que, "es esencial definir una serie de normas que consideren las acciones automatizadas y su efecto en la responsabilidad legal". Esto abarca no solo el establecimiento de normativas que controlen la aplicación de la IA, sino también la elaboración de principios que orienten la distribución de responsabilidad en circunstancias donde las acciones son el producto de procesos automatizados.

La noción de acción ha progresado en la época digital, cuestionando las definiciones convencionales y proponiendo nuevos conflictos legales. La interrelación entre seres humanos y maquinaria ha generado desafíos que demandan un enfoque renovado en la responsabilidad y la atribución de acciones. La incorporación de la Inteligencia Artificial en la toma de decisiones enfatiza la necesidad de marcos regulatorios que identifiquen esta nueva realidad, facilitando un entendimiento más integral de cómo se establece la acción en un mundo digital. Solo mediante esta modificación podremos garantizar que el

derecho continúe desempeñando su papel de salvaguardar y regular el comportamiento en un contexto donde la tecnología tiene un rol crucial.

La Inteligencia Artificial en crímenes financieros, desde los principios del derecho penal

El lavado de activos (artículo 323 del Código Penal en colombiano) conlleva la transformación o transferencia de bienes provenientes de actividades ilegales con el objetivo de esconder u ocultar su procedencia. La financiación del terrorismo (artículo 345 del Código Penal colombiano) implica la aportación o recopilación de recursos para acciones terroristas. Los dos delitos son examinados como graves debido a sus impactos en el orden económico y social, y su carácter transfronterizo los transforma en un reto para los sistemas penales convencionales. La implementación de Inteligencia Artificial en estos crímenes incrementa la complejidad de las operaciones y la habilidad para eludir los sistemas de detección tradicionales, lo que provoca la demanda de respuestas regulatorias más avanzadas.

La Piedra Angular de la Justicia en un Estado de Derecho

El principio de legalidad, definido en el artículo 9 del Pacto Internacional de Derechos Civiles y Políticos e incorporado en diversos sistemas penales, sostiene que no existe crimen ni castigo sin una ley anterior que lo establezca (nullum crimen, nulla poena sine lege). Este principio constituye una protección ante la arbitrariedad del poder de sanción del Estado. Dentro del marco de los crímenes realizados con la Inteligencia Artificial, se presenta el desafío de modificar las leyes vigentes para tener en cuenta las nuevas modalidades delictivas que surgen con el progreso tecnológico. (Zaffaroni, 2021) en su doctrina, indica que "la legislación penal debe ser nítida y exacta para que los ciudadanos tengan la certeza de qué comportamientos están prohibidos". Este principio exige a los legisladores prever las formas delictivas propiciadas por la tecnología, asegurando que la Inteligencia Artificial no produzca vacíos legales que puedan ser aprovechados.

La implementación de la Inteligencia Artificial en crímenes como el blanqueo de capitales y la financiación del terrorismo representa un reto directo al principio de legalidad, por diversos motivos, entre otros:

Indeterminación tecnológica: Las normativas criminales vigentes no siempre contemplan la aplicación de tecnologías de vanguardia como la Inteligencia Artificial, lo que podría generar lagunas legales o interpretaciones confusas.

Responsabilidad penal y autonomía de la IA: La asignación de responsabilidad es un elemento crucial del principio de legalidad. Cuando se emplea Inteligencia Artificial en la perpetración de un crimen, se plantea la interrogante de si el creador, el operador o el usuario final son los responsables penales. (Roxin C. , 1997) argumenta que el principio de legalidad requiere que la responsabilidad penal sea asignada exclusivamente a individuos que ejercen un control consciente sobre el comportamiento delictivo. La Inteligencia Artificial, al comportarse de forma autónoma en determinados escenarios, dificulta esta atribución.

Requerimiento de exactitud legislativa: La implementación de Inteligencia Artificial en el lavado de activos y la financiación del terrorismo demanda que las normativas sean lo suficientemente exactas para incluir estas nuevas formas de delincuencia. En este contexto, Claus Roxin sostiene que "la exactitud en la definición de los tipos penales es crucial para prevenir interpretaciones amplias que infrinjan el principio de legalidad" (Roxin C. , 1997).

El principio de legalidad, fundamental para salvaguardar los derechos personales en el ámbito penal, se embiste con retos considerables en el marco de los crímenes de lavado de dinero y financiación del terrorismo realizados mediante la utilización de inteligencia artificial. Es necesario modificar las leyes penales para incorporar estas nuevas formas de delincuencia, garantizando el respeto a los principios de certeza, claridad y previsibilidad. En este contexto, el desafío no solo es técnico, sino también regulatorio, ya que la penalización debe adaptarse a las circunstancias tecnológicas actuales sin poner en riesgo los principios esenciales del derecho.

Equilibrio entre castigo y conducta en la era de la IA

El concepto de proporcionalidad se fundamenta en la noción de que la penalización debe ajustarse a la severidad del delito y al perjuicio provocado. Respecto a los crímenes de lavado de dinero y financiación del terrorismo, tomar especial importancia los planteado

por (Roxin C. , 1997) que indica que la sanción debe mantener una "conexión lógica entre la infracción perpetrada y el castigo impuesto, de manera que no se altere el balance entre el interés del Estado en sancionar y los derechos esenciales del individuo".

Cuando se cometen estos delitos mediante la utilización de Inteligencia Artificial, la implementación de este principio demanda analizar la complejidad y sofisticación añadida por la tecnología. Por ejemplo, si se emplea la IA para automatizar procedimientos financieros que esconden activos ilegales en diversas jurisdicciones, la penalización debería adaptarse a la severidad adicional que la tecnología aporta. No obstante, esta avanzada tecnología no debe convertirse automáticamente en castigos más rigurosos sin un estudio minucioso del contexto y la implicación del imputado en la utilización de la IA.

Justificando la intervención penal en tiempos de innovación tecnológica

El principio de necesidad sostiene que la sanción solo debe aplicarse cuando sea absolutamente necesaria para salvaguardar los bienes jurídicos en peligro. (Jakobs, 2016) sostiene que, "el derecho penal debe ser el último recurso, o sea, el último nivel de control social cuando otros procedimientos han fallado". En crímenes en los que se emplea la Inteligencia Artificial para realizar lavado de dinero o financiar el terrorismo, es vital que las sanciones penales no se impongan de forma selectiva. El derecho penal debe actuar cuando las acciones preventivas, normativas o administrativas no bastan para prevenir la perpetración de estos crímenes. En algunas situaciones, la IA puede provocar dudas sobre la responsabilidad penal de los participantes involucrados (desarrolladores, operadores o usuarios), lo que requiere un estudio minucioso de si la penalización es verdaderamente necesaria y dirigida al individuo adecuado.

En crímenes como el blanqueo de capitales y la financiación del terrorismo, cuando se utiliza inteligencia artificial, resulta vital establecer si se requiere una acción penal. La Inteligencia Artificial puede simplificar la automatización de actividades ilegales, sin embargo, el derecho penal debe actuar únicamente cuando las acciones regulatorias o administrativas no bastan. (Zaffaroni, 2021) alerta que se debe valorar meticulosamente la necesidad de sanción para prevenir abusos del poder punitivo, en particular frente a tecnologías que pueden dificultar la imputación de responsabilidad.

La búsqueda del justo medio entre normativa y realidad en la era digital

El principio de razonabilidad requiere que las sanciones aplicadas sean equitativas y no excesivas en su gravedad o uso. Este precepto tiene una conexión directa con la dignidad humana, tal como lo reconocen mecanismos internacionales como la Convención Americana sobre Derechos Humanos; En este escenario, la razonabilidad significa considerar el empleo de la Inteligencia Artificial como una situación que puede intensificar o disminuir la responsabilidad penal, en función del grado de control y entendimiento que el imputado poseía acerca del funcionamiento del sistema de IA. (Suarez, 2022) indica que, "cuando la Inteligencia Artificial tiene un rol significativo en la comisión del delito, resulta crucial valorar el grado de participación humana y si la IA se empleó con conocimiento y decisión". Por lo tanto, una persona que emplea Inteligencia Artificial con el propósito de esconder activos ilícitos podría enfrentar una sanción más rigurosa, mientras que un individuo que no mantiene un control directo sobre el sistema de IA podría obtener una penalización más suave.

La penalización en los crímenes de lavado de dinero y financiación del terrorismo realizados mediante la aplicación de inteligencia artificial debe acatar los principios esenciales del derecho penal: legalidad, proporcionalidad, necesidad y razonabilidad. La Inteligencia Artificial no solo cambia el modo en que se cometen estos delitos, sino que también requiere una modificación de los marcos legales y de sanciones para prevenir que esta tecnología se transforme en un instrumento de impunidad. El derecho penal debe preservar su papel de salvaguarda de los bienes jurídicos y, simultáneamente, tener la flexibilidad necesaria para adaptarse a las nuevas realidades tecnológicas sin infringir las garantías esenciales de los imputados. Como propone (Zaffaroni, 2021) el porvenir del derecho penal ante la tecnología se basará en su habilidad para continuar salvaguardando de forma eficiente y equitativa los bienes jurídicos de mayor relevancia sin incurrir en excesos sancionatorios.

Revolución digital: la urgente necesidad de modernizar la legislación penal para regular las conductas en la era de la inteligencia artificial

El rápido y vertiginoso avance de la inteligencia artificial ha revolucionado varias áreas sociales, entre ellas la comisión de crímenes. Estas tecnologías posibilitan la

automatización y mejora de actividades ilegales, complicando la persecución penal de comportamientos que, a pesar de no haber sufrido cambios fundamentales, se ven simplificados por la utilización de instrumentos tecnológicos de vanguardia. Delitos como el blanqueo de capitales y la financiación del terrorismo, que ya representan una seria amenaza para la estabilidad económica y pública, cobran una nueva dimensión cuando se llevan a cabo a través de la IA.

La IA ha permitido la automatización de labores que antes necesitaban de la participación humana, originando así nuevas modalidades de delincuencia. De acuerdo con (Zaffaroni, 2021), el progreso tecnológico requiere una "adaptación continua del derecho penal para prevenir vacíos legales que podrían ser aprovechados por los delincuentes". Esto es especialmente significativo en los delitos financieros, donde la Inteligencia Artificial tiene la capacidad de ocultar la identidad de los delincuentes, generar patrones avanzados de operaciones ilícitas y eludir sistemas de control tradicionales.

El principio de lex certa o legalidad penal requiere que los comportamientos sean claramente establecidos en la ley para prevenir la arbitrariedad. Sin embargo, (Jakobs, 2016) alerta que la legislación no puede anticipar todas las maneras en que las tecnologías emergentes pueden emplearse en acciones delictivas. Así pues, resulta esencial renovar las leyes para afrontar estas nuevas formas de delincuencia sin incurrir en generalizaciones riesgosas que transgreden el principio de certeza legal.

En la actualidad, la mayoría de las legislaciones penales no contemplan de manera explícita la comisión de crímenes a través de Inteligencia Artificial. Esto crea un hueco que puede ser utilizado por actores delictivos que emplean la tecnología para perpetrar crímenes sin tener que confrontar una regulación apropiada. (Roxin C. , 1997) argumenta que "las leyes penales deben adaptarse a las transformaciones sociales y tecnológicas, sin poner en riesgo los derechos esenciales de los imputados". La ausencia de previsión legislativa puede generar circunstancias en las que los delitos perpetrados con Inteligencia Artificial sean complicados de penalizar, no por la ausencia de culpabilidad, sino porque el comportamiento no está claramente categorizado.

Por ejemplo, en lo que respecta al lavado de activos, la Inteligencia Artificial puede emplearse para automatizar procedimientos de ocultación de activos ilegales a través de

diversas jurisdicciones en tan solo unos segundos. Sin un marco normativo apropiado, estos comportamientos pueden resultar complicados de seguir y penalizar. Asimismo, en el financiamiento del terrorismo, la Inteligencia Artificial tiene la capacidad de optimizar flujos económicos mediante criptomonedas o deepfakes que imiten identidades verdaderas para simplificar el envío de recursos a organizaciones terroristas sin ser identificadas.

Es imprescindible y urgente la actualización de la legislación penal para abordar el reto que implica el empleo de la inteligencia artificial en la comisión de crímenes como el blanqueo de capitales y la financiación del terrorismo. Esta actualización no solo debe clasificar correctamente las nuevas modalidades delictivas, sino también asegurar que las penalizaciones sean justas y honren los principios esenciales del derecho penal, tales como la legalidad y la proporcionalidad. Autores como Zaffaroni, Roxin y Floridi están de acuerdo en que el progreso normativo es crucial para garantizar la efectividad del sistema penal en un escenario de rápidos progresos tecnológicos.

Contribución de la inteligencia artificial al derecho penal

La inteligencia artificial ha probado ser un instrumento innovador en varias disciplinas del saber, incluyendo el derecho penal. Su habilidad para manejar grandes volúmenes de información, detectar patrones complejos y producir pronósticos sólidos tiene el potencial de modificar de manera significativa la manera en que se previenen, investigan y castigan los delitos. No obstante, la implementación de la Inteligencia Artificial en este sector también presenta retos éticos, reglamentarios y técnicos que requieren un tratamiento meticuloso.

Una de las contribuciones más significativas de la Inteligencia Artificial al derecho penal reside en su uso en la identificación temprana de comportamientos delictivos. Los sistemas sofisticados de análisis predictivo tienen la capacidad de detectar patrones de conducta vinculados a actividades ilegales, como el blanqueo de capitales o la financiación del terrorismo, al examinar grandes cantidades de información en tiempo real. De acuerdo con (Hallevy, 2013), "los algoritmos de aprendizaje automático son capaces de detectar correlaciones que los investigadores humanos ignoraban,

ofreciendo de esta manera un beneficio considerable en la batalla contra el crimen organizado".

En el contexto procesal, la Inteligencia Artificial puede mejorar la investigación y recopilación de evidencias, facilitando a las autoridades el manejo de información de forma más eficaz. Por ejemplo, herramientas fundamentadas en Inteligencia Artificial pueden examinar horas de grabaciones de cámaras de vigilancia o examinar miles de documentos jurídicos para detectar pruebas significativas en un caso. De acuerdo con (PASQUALE, 2015), "la Inteligencia Artificial posee la capacidad de disminuir considerablemente el tiempo y los gastos relacionados con las investigaciones delictivas, sin poner en riesgo la calidad de los hallazgos".

Igualmente, la Inteligencia Artificial puede aportar al robustecimiento de la justicia penal a través de la creación de sistemas de evaluación de riesgos. Estos sistemas tienen la capacidad de estimar la posibilidad de reincidencia de un imputado, lo que facilita a los operadores judiciales, la toma de decisiones más fundamentadas respecto a medidas preventivas, fallos o libertad condicional. No obstante, (Floridi, 2013) alerta acerca de la importancia de asegurar que los algoritmos empleados sean transparentes, equitativos y no perpetúen prejuicios discriminatorios, dado que cualquier error en su diseño o aplicación podría poner en riesgo los principios de equidad y justicia.

Pese a estos beneficios, la aplicación de la Inteligencia Artificial en el ámbito penal presenta retos significativos. Por un lado, se presenta la necesidad de renovar los marcos regulatorios para regular su aplicación, asegurando que su empleo respete los derechos esenciales y los principios fundamentales del derecho penal, tales como la presunción de inocencia y el debido proceso. Por otro lado, es necesario un control estricto sobre la calidad y la ética de los algoritmos utilizados, dado que, como indica (Floridi, 2013), "la opacidad intrínseca de ciertos sistemas de Inteligencia Artificial representa el peligro de decisiones automatizadas que no pueden ser explicadas o entendidas completamente".

Como lo plantea (Lozano, 2024), la inteligencia artificial brinda una contribución significativa al derecho penal, no solo incrementando la eficacia en la investigación y persecución del crimen, sino también proporcionando instrumentos que fomenten decisiones mejor fundamentadas y justas. Sin embargo, su incorporación debe estar

respaldada por un sólido marco regulatorio y una perspectiva ética que asegure su uso responsable. Solo a través de un balance entre la innovación tecnológica y la salvaguarda de derechos esenciales podremos potenciar las ventajas de la IA en el campo penal.

Finalmente, es importante destacar que, como lo propone (UIBERO, 2025) la revolución digital ha cambiado radicalmente el contexto en el que se perpetran y norman los delitos, presentando desafíos significativos para el derecho penal. Las tecnologías en auge, como la inteligencia artificial, el big data y el blockchain, han propiciado el surgimiento de nuevos tipos de delitos, tales como el cibercrimen, el lavado de activos a través de criptomonedas y la financiación del terrorismo por medio de plataformas digitales. Este escenario requiere una revisión y renovación de los marcos regulatorios para asegurar una respuesta legal eficaz y adecuada a los retos de la era tecnológica.

Asimismo, se deduce que el derecho penal se tropieza con una laguna normativa importante en la regulación de comportamientos ilícitos relacionados con el uso de tecnologías de punta. Las reglas convencionales, creadas para responder a crímenes tradicionales, no toman en cuenta la complejidad de los crímenes digitales ni la participación de elementos no humanos, como los algoritmos y sistemas de inteligencia artificial. Esto demanda una legislación flexible que contemple las especificidades de los ambientes digitales.

Por otro lado, es necesario reformular la responsabilidad penal para tratar la implicación de tecnologías autónomas en la perpetración de crímenes. A diferencia del derecho penal convencional donde la imputación se fundamenta en la voluntad y la acción humana, la revolución digital presenta situaciones donde las máquinas desempeñan el papel de ejecutores. Esto requiere definir estándares precisos para asignarle responsabilidades a los desarrolladores, operadores o usuarios de estas tecnologías, tal como propone (Hallevy, 2013).

Otro reto principal detectado es la importancia de mantener los principios esenciales del derecho penal, tales como la legalidad, proporcionalidad, razonabilidad y necesidad, en un contexto donde la rapidez y el alcance de las tecnologías digitales pueden propiciar decisiones automatizadas que perjudiquen derechos esenciales. (Floridi, 2013) alerta

que la aplicación de sistemas de inteligencia artificial en procedimientos judiciales debe asegurar la transparencia y la responsabilidad, previniendo prejuicios discriminatorios y asegurando el debido proceso.

Respecto a las soluciones, se sugiere el establecimiento de marcos normativos internacionales que traten los delitos digitales de forma homogénea, debido a su naturaleza transfronteriza. Además, se sugiere la capacitación interdisciplinaria para los profesionales del jurídicos, fusionando saberes en derecho y tecnología, para manejar de manera eficiente la complejidad de los casos digitales. Finalmente, la implementación de tecnologías como la Inteligencia Artificial también surge como una oportunidad para potenciar la investigación y la persecución de crímenes. No obstante, su aplicación debe estar regida por principios éticos que den prioridad a la salvaguarda de los derechos humanos y a la certeza legal.

Finalmente, el derecho penal en la revolución digital se encuentra con el reto de ajustarse a un ambiente tecnológico que cambia continuamente, asegurando que las medidas jurídicas no solo sean eficaces, sino también respetuosas con los principios básicos. Será esencial la armonización entre la innovación tecnológica y las regulaciones legales para enfrentar los delitos de la era tecnológica con equidad y justicia.

Bibliografía

Azuaje Pirela, M., & Contreras, P. (2021). *Inteligencia artificial y derecho - desafíos y perspectivas.* España: Tirant lo Blanch.

Castellà Andreu, J., Montobbio, M., & Granata-Menghini, S. (2022). *Estado de derecho, democracia y globalización.* Madrid: Centro de Estudios Políticos y Constitucionales. Obtenido de https://www.cepc.gob.es/sites/default/files/2022-09/a-1035-estadoaccesible-ok.pdf

Chen Cheng , C., Chung , E., & Correa , N. (2023). La inteligencia Artificial y su Impacto en la Industria de la Ingeniería. *Revista especializada de ingenierias y cicencias de la tierra*. Obtenido de https://d1wqtxts1xzle7.cloudfront.net/104828215/3330-libre.pdf?1691420427=&response-content-disposition=inline%3B+filename%3Dinteligencia_Artificial_y_su_Impacto_en.pdf&Expires=1736529115&Signature=RBmTxOJcIZQYQFsVwPOxL7RcULCndXG5MFj7nGhjjFeJNQheu7a6bx3LN

Compliance. (s.f.). Inteligencia Artificial una herramienta para prevenir el Lavado de Activos e identificar beneficiarios finales. Obtenido de https://www.compliance.com.co/inteligencia-artificial-una-herramienta-para-prevenir-el-lavado-de-activos-e-identificar-beneficiarios-finales/

Erdélyi, O., & Goldsmith, J. (2022). Regulación de la inteligencia artificial: propuesta para una solución global. *ScienceDirect*. Obtenido de https://www.sciencedirect.com/science/article/abs/pii/S0740624X22000843

Espinosa, A. M. (2021). Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera? *Revista IUS*, 289-323. Obtenido de https://www.scielo.org.mx/scielo.php?pid=S1870-21472021000200289&script=sci_abstract&tlng=es

Financial Crime Academy. (6 de 1 de 2025). Las aplicaciones de la IA en KYC. Obtenido de https://financialcrimeacademy.org/es/las-aplicaciones-de-la-ia-en-kyc/

Floridi, L. (2013). *The Ethics of Information.* Oxford: Universidad de Oxford.

González Arencibia, M., & Martínez Cardero, D. (2020). Dilemas éticos en el escenario de la inteligencia artificial. *Economía y Sociedad*. Obtenido de https://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S2215-34032020000100093

Hallevy, G. (2013). *When Robots Kill: Artificial Intelligence Under Criminal Law.* Toronto: Northeastern Univ Pr.

J. Russell, S., & Norvig, P. (2020). *Artificial Intelligence A Modern Approach.* Pearson. Obtenido de https://people.engr.tamu.edu/guni/csce421/files/AI_Russell_Norvig.pdf

Jakobs, G. (2016). *Teoría de la intervención.* Universidad Externado de Colombia.

Kelsen, H. (1960). *Teoría Pura del Derecho.* Buenos Aires: Editorial Universitaria de Buenos Aires .

Lessig, L. (2006). *Código 2.0.* Madrid: Traficantes de Sueños. Obtenido de https://www.articaonline.com/wp-content/uploads/2011/07/El-c%C3%B3digo-2.0-Lawrence-Lessig.pdf

Lozano, D. (2024). Inteligencia artificial en el derecho penal, una discusión sobre su uso en el sistema jurídico colombiano.

LUÑO, A.-E. P. (2012). El derecho ante las nuevas tecnologías. *Notario del siglo XXI*. Obtenido de https://www.elnotario.es/index.php/hemeroteca/revista-41/548-el-derecho-ante-las-nuevas-tecnologias-0-8050094412686392

Meseguer, P. (2023). *Inteligencia artificial: retos y oportunidades.* CyD. Obtenido de https://www.fundacioncyd.org/wp-content/uploads/2023/12/G-MONOGRAFIA-ICYD23.pdf

Metaverso. (s.f.). *Metaverso Pro*. Obtenido de https://metaverso.pro/blog/autonomia-y-responsabilidad-en-la-era-de-la-inteligencia-artificial/

Moreno, V. A. (2024). La Protección de Datos y el avance tecnológico. *Blog Jurídico - TECH*. Obtenido de https://telecomunicaciones.uexternado.edu.co/la-proteccion-de-datos-y-el-avance-tecnologico/

PASQUALE, F. (2015). *The black box society.* Londres: Cambridge. Obtenido de https://raley.english.ucsb.edu/wp-content/Engl800/Pasquale-blackbox.pdf

Porcelli, A. M. (2020). La inteligencia artificial y la robótica: sus dilemas sociales, éticos y jurídicos. *Derecho global. Estudios sobre derecho y justicia*. Obtenido de https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2448-51362020000300049

Rincón Arteaga, J., Castiblanco Hernández, S., Quijano Díaz, A., Urquijo Vanegas, J., & Pregonero León, Y. (2023). Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos? *Revista Criminalidad*. Obtenido de http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082022000300095

Roxin, C. (1997). *Derecho Penal, Parte General.* Madrid: Civitas S.A.

Roxin, C. (2006). *Dependencia e independencia del derecho penal con respecto a la politica, la filosofia, la religion y la moral.* Madrid: ADPCP.

Sanchez, M., & Caicedo, L. (s.f.). Nuevas tecnologías en IA para la prevención del LA/FT. Obtenido de https://www.compliance.com.co/nuevas-tecnologias-en-ia-para-la-prevencion-del-la-ft/

Sayad, A. L. (2023). *INTELIGENCIA ARTIFICIAL Y PENSAMIENTO CRITICO.* Sao Paulo: UNIMINUTO. Obtenido de https://repository.uniminuto.edu/server/api/core/bitstreams/a8a92c98-2339-4acb-a453-f249c27cb4bd/content

Suarez, M. F. (2022). Inteligencia Artificial y Derecho Penal. *Pensamiento Penal*.

UIBERO. (2025). El impacto de la Inteligencia Artificial en el Derecho: ¿amenaza o aliado? *Corporación Universitaria Iberoamericana*.

Universidad del Bosque. (s.f.). Derecho y tecnología: entre la ley y la innovación digital. Bogotá, Colombia. Obtenido de https://www.unbosque.edu.co/blog-universidad-el-bosque/derecho-y-tecnologia-entre-la-ley-y-la-innovacion-digital

Verdegay , J., Lamata, M., Pelta, D., & Cruz, C. (2021). Inteligencia artificial y problemas de decisión: la necesidad de un contexto ético. *Suma de Negocios*, 104-114. Obtenido de https://www.redalyc.org/journal/6099/609970431002/html/

Zaffaroni, E. R. (2021). La criminología crítica de la justicia penal, de ayer y de hoy. *Revista Crítica Penal y Poder*, 60-63. Obtenido de https://revistes.ub.edu/index.php/CriticaPenalPoder/article/view/37112/35940