

Aplicación de la inteligencia artificial en el Derecho Penal: problemas y desafíos

Challenges and Opportunities in Implementing Artificial Intelligence in Criminal Law

María Paula Ávila Zea, Ana Fabiola Zamora Vázquez

RESUMEN

La integración de la tecnología en el ámbito del derecho penal plantea desafíos significativos debido a la falta de regulación de la inteligencia artificial (IA), lo que podría comprometer los derechos fundamentales. Este estudio se centra en abordar estos desafíos y proponer soluciones mediante un análisis exhaustivo de la situación actual y las posibles implicaciones de la IA en el sistema jurídico penal. El objetivo principal de esta investigación es analizar los problemas, desafíos y oportunidades que surgen con la implementación de la inteligencia artificial en el ámbito penal. Se busca identificar la necesidad de una regulación específica para la IA en el derecho penal, con el fin de proteger los derechos fundamentales de las personas y garantizar un sistema jurídico justo y equitativo. Para abordar esta problemática, se adoptó un enfoque metodológico cualitativo. Se llevó a cabo una revisión bibliográfica detallada para examinar los antecedentes, problemas y desafíos asociados con la IA en los sistemas jurídicos, especialmente en el ámbito penal. Además, se realizaron análisis de criterios y opiniones de expertos en derecho para obtener una comprensión más profunda de la situación y las posibles soluciones. Los resultados de este estudio revelan la necesidad urgente de establecer una normativa específica para regular la aplicación de la inteligencia artificial en el ámbito penal. Se destaca que la falta de regulación representa un riesgo significativo para los derechos fundamentales, especialmente en lo que respecta a la configuración de delitos con el apoyo de la IA. Además, se identifican diferentes dimensiones que deben abordarse en la regulación, incluyendo principios y reglas básicas del derecho, supervisión humana de los sistemas de IA y la promoción de la innovación responsable en este campo. Este artículo subraya la importancia de establecer una regulación efectiva para la inteligencia artificial en el ámbito penal. Esta regulación no solo protegerá los derechos fundamentales de las personas, sino que también promoverá un uso responsable y progresivo de la IA como una herramienta valiosa para los profesionales del derecho. Es crucial que la regulación sea integral y adaptable para garantizar un sistema jurídico justo y equitativo en la era digital.

Palabras clave: Inteligencia artificial; cambio social; tecnología; delito informático; digitalización; derecho.

María Paula Ávila Zea

Universidad Católica de Cuenca | Cuenca | Ecuador. mpavilaz93@est.ucacue.edu.ec

<http://orcid.org/0009-0000-6596-2807>

Ana Fabiola Zamora Vázquez

Universidad Católica de Cuenca | Cuenca | Ecuador. afzamorav@ucacue.edu.ec

<http://orcid.org/0000-0002-1611-5801>

<http://doi.org/10.46652/resistances.v5i9.142>

ISSN 2737-6230

Vol. 5 No. 9 January-June 2024, e240142

Quito, Ecuador

Submitted: december 18, 2023

Accepted: february 27, 2024

Published: march 14, 2024

Continuous Publication

ABSTRACT

The integration of technology in the field of criminal law poses significant challenges due to the lack of regulation of artificial intelligence (AI), which could compromise fundamental rights. This study focuses on addressing these challenges and proposing solutions through a comprehensive analysis of the current situation and potential implications of AI in the criminal legal system. The main objective of this research is to analyze the problems, challenges and opportunities that arise with the implementation of artificial intelligence in the criminal field. It seeks to identify the need for a specific regulation for AI in criminal law, to protect the fundamental rights of individuals and ensure a fair and equitable legal system. To address this issue, a qualitative methodological approach was adopted. A detailed literature review was carried out to examine the background, problems and challenges associated with AI in legal systems, especially in the criminal field. In addition, analyses of criteria and opinions of legal experts were conducted to obtain a deeper understanding of the situation and possible solutions. The results of this study reveal the urgent need to establish specific regulations to govern the application of artificial intelligence in the criminal field. It is highlighted that the lack of regulation represents a significant risk to fundamental rights, especially regarding the configuration of crimes with the support of AI. In addition, different dimensions that need to be addressed in regulation are identified, including basic principles and rules of law, human oversight of AI systems, and the promotion of responsible innovation in this field. This article highlights the importance of establishing effective regulation for artificial intelligence in the criminal sphere. Such regulation will not only protect the fundamental rights of individuals, but also promote responsible and progressive use of AI as a valuable tool for legal professionals. It is crucial that the regulation be comprehensive and adaptive to ensure a fair and equitable legal system in the digital age.

Keywords: Artificial intelligence; social change; technology; computer crime; digitization; law.

Introducción

El avance de la tecnología ha transformado el mundo, haciendo que las personas cambien su estilo de vida para adaptarse a la nueva era digital que estamos atravesando, asumiendo nuevas necesidades y problemas. El surgimiento de la inteligencia artificial en el derecho ha ocasionado cambios significativos en cada una de sus ramas, en donde los profesionales del derecho van a enfrentarse a diferentes desafíos, en especial en el campo penal, por lo que se exige el máximo de adaptabilidad en los sistemas normativos (Parra Sepúlveda, 2021).

En este marco, la presente investigación surge con el propósito de estudiar íntegramente a la inteligencia artificial en el derecho penal, a través de análisis de casos en donde se encuentra involucrada la misma. Sin embargo, la ausencia de ley obliga a los profesionales del derecho dar soluciones conforme a normativa existente, derecho comparado y jurisprudencia, dando lugar a problemas jurídicos complejos y globales (Frosini, 2019). Por lo que, resulta necesario hacer una reflexión al derecho actual y diseñar un sistema normativo que se adapte a nuevas relaciones jurídicas.

Todo esto con la finalidad que el ordenamiento jurídico avance juntamente con la tecnología, en virtud que se van a configurar delitos en donde que se encuentre implicada la inteligencia artificial y se deberá encontrar al responsable de esa conducta ilícita, puesto que detrás de cada método tecnológico existirá un autor intelectual de dicho algoritmo.

Es relevante analizar a la inteligencia artificial en el campo penal por varios motivos, que generan problemas y desafíos como es: transparencia al momento de tomar decisiones judiciales, evitar discriminación algorítmica, retos éticos y legales para garantizar que los sistemas sean seguros y no perpetúen discriminaciones, así como también la protección de datos y privacidad. Además, la ausencia de normativa puede desencadenar la vulneración de derechos fundamentales consagrados en la Constitución de la República del Ecuador y demás cuerpos normativos.

El objetivo de la investigación es analizar los problemas, desafíos y oportunidades que surgen con la implementación de la inteligencia artificial en el ámbito penal. Se propone normativa que regule en derecho penal para evitar conflictos de leyes o vacíos legales. La pregunta de investigación establece ¿Cuáles son los problemas, desafíos y oportunidades que presenta la aplicación de la inteligencia artificial en el ámbito penal y como puede influir en las decisiones judiciales?

Esta era digital cuenta con beneficios y oportunidades para los profesionales del derecho que pretenden ser de gran ayuda al mejorar la eficiencia de los servidores legales y asesoramientos jurídicos. Sin embargo, no se debe olvidar que todo esto debe ser regulado por normativa, puesto que, de no ser así, quebrantaría el ordenamiento jurídico y vulneraría derechos fundamentales.

Ante esta situación, es importante comprender el comportamiento de la sociedad, para que, de esa manera, se implemente normativa conforme a las nuevas necesidades. Esto con el propósito de que las personas utilicen sistemas tecnológicos, de manera responsable. Por lo que, se requiere una regulación a los posibles retos y desafíos que se van a presentar en el transcurso del tiempo y de esta manera evitar problemas en los sistemas judiciales.

Con base a lo mencionado, este estudio aborda antecedentes, definiciones y fundamentos teóricos sobre la inteligencia artificial desde una perspectiva jurídica. Posteriormente, se analizarán los problemas, retos y desafíos que surgen con la implementación de la inteligencia artificial desde el ámbito penal. Además, se examinarán las oportunidades que ofrece a todos los profesionales del derecho y finalmente se realizará una propuesta de ley que regule el uso de la inteligencia artificial en el derecho.

Marco Teórico

Inteligencia Artificial

La inteligencia artificial en adelante (IA) es una rama de la ciencia informática que se define como la combinación de algoritmos que posibilita la creación de máquinas automatizadas para resolver problemas de forma rápida y efectiva expertas en un ámbito concreto, al igual, analizar datos, actualizar conocimientos, así como realizar tareas similares a los seres humanos esto con fundamento en la propuesta de la Comisión Mundial de Ética del Conocimiento Científico y la Tecnología de la UNESCO (Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, 2020).

Los sistemas con IA utilizan neurociencias y demás métodos tecnológicos para lograr que una máquina se comporte como un humano, esto es, con una serie de cualidades y capacidades, como pensar, razonar, actuar, distinguir, adaptarse, resolver problemas, entre otros rasgos. Para ello, se requiere del área de especialización con el propósito de que, pueda interactuar en su entorno con un pensamiento lógico, racional y con la intervención mínima de las personas.

El enfoque de la IA es imitar la inteligencia humana a través de procedimientos computarizados, así como tener la capacidad de adquirir funciones cognitivas que poseen las personas, tal como, aprender y razonar. En este sentido, es necesario estudiar a la IA desde dos áreas. La primera es la ciencia cognitiva que consiste en estudiar la inteligencia humana, su mente, su forma de hablar e interactuar para así lograr descifrar sus habilidades y resolver problemas con gran rapidez, esto con la finalidad de que una máquina cuente con las mismas capacidades. La segunda es las ciencias formales e ingenierías, cuya función es aplicar los conocimientos que han adquirido, por medio de la creación de artefactos para que puedan trabajar en cualquier especialidad (Parra Sepúlveda, 2021).

Se centra en estas dos disciplinas, aunque su finalidad va a ser adquirir autonomía al igual que autodependencia, así como también, ser auto adaptativa. Todo esto por medio del manejo de técnicas para el reconocimiento de patrones de modo que puedan resolver conflictos, cumplir metas, optimizar tiempo y procesar información a través de la codificación, almacenamiento y recuperación de datos.

Los sistemas de IA se clasifican de acuerdo con sus niveles de riesgo para localizar los posibles daños que puedan afectar los bienes jurídicos protegidos. Con la finalidad de prevenir la vulneración de derechos fundamentales reconocidos en la Constitución de la República y demás cuerpos normativos. La Comisión Europea establece cuatro niveles de riesgo en su propuesta de legislación porque cuando mayor es el riesgo, más exigente tiene que ser la ley, estos son:

Los sistemas de IA, con riesgo inaceptable, tienen un alto índice de peligrosidad y su utilización se encuentra prohibida, salvo casos previstos en la ley. Esto es, cuando se vulnera el derecho de privacidad, se podrá emplear algoritmos para garantizar la protección de datos e información personal. Además, se podrá emplear para fines de seguridad nacional. Ejemplo, robo de identidad a través de deepfakes, vigilancia masiva para cometer delitos de robo, bots ladrones y demás delitos (Martínez Espín, 2023).

Los sistemas de alto riesgo se encuentran sometidos a constantes evaluaciones con el propósito de examinar los patrones de información para proteger la privacidad y la no discriminación. Además, se buscará la transparencia en el uso de datos que ha sido proporcionada por los usuarios, teniendo como propósito, disminuir riesgos y proteger datos a causa de que pueda ser utilizada de manera inadecuada. Ejemplo, cámaras de reconocimiento facial o vigilancia biométrica.

Los sistemas de riesgo limitado, minimiza los daños que pueda generar, aunque no los descarta. Obliga a los usuarios a utilizarla con transparencia y responsabilidad, puesto que las personas son conscientes que están interactuando con máquinas. Ejemplo: publicidad online, asistente virtual. Por último, se encuentran los sistemas de IA que tienen un nivel de riesgo mínimo, este se emplea a través de chat bots, de modo que podrán realizar tareas, consultas, resolver inquietudes y demás aplicaciones que sean habilitados para la IA. Ejemplo Chat GPT.

Los sistemas con IA que tengan un nivel de riesgo alto o inaceptable son sujetos a fiscalización, puesto que, son más propensos a causar daño y vulnerar derechos fundamentales. se debe regular con normativa específica que establezca sus requisitos y prohibiciones, caso contrario, se encuentra en peligro el derecho a la seguridad debido a que, se podrá crear o manipular imágenes, videos, audios a fin de causar daño a un tercero.

La Comisión Europea, afirma que los medios tecnológicos han dejado de ser una ciencia ficción para convertirse en un estilo de vida. Su crecimiento en capacidad informática, la disponibilidad de datos como los avances cibernéticos algorítmicos han convertido a la IA en una herramienta estratégica e innovadora del siglo XXI. (Comisión Europea, 2018).

Los cambios que está viviendo la sociedad, por la tecnología, es alarmante. Por lo tanto, la forma en que se aborde el tema de la IA definirá el mundo en el que vamos a vivir. Los organismos internacionales, como la Unión Europea, ha lanzado una propuesta de un sistema normativo que regule el desarrollo de la IA. En este sentido, los siguientes apartados estarán enfocados en analizar a la IA desde una perspectiva jurídica penal.

Inteligencia artificial en el Derecho

La integración de máquinas con la codificación de sistemas expertos jurídicos, capaces de resolver problemas legales y tomar decisiones de forma autónoma, traerá consigo consecuencias jurídicas. Es necesario realizar un análisis centrado en el derecho y los avances tecnológicos debido a que, la IA está transformando el sistema jurídico. En donde los problemas se han comenzado a expandir en distintas áreas del ordenamiento jurídico. No obstante, aún no se ha logrado crear un cuerpo normativo específico para la IA en donde se incluya principios, normas y reglas (Solar Cayón, 2020).

La rápida evolución de la tecnología ha traído como desafío a la IA en el ámbito jurídico; sin embargo, se debe analizar este problema desde un enfoque multidisciplinario y avanzar juntamente con el derecho y la tecnología. Solo así se tendrán resultados positivos para garantizar el bienestar a la sociedad, siendo esto la finalidad de todo Estados de derechos.

Los profesionales del derecho deben prepararse para resolver nuevas cuestiones legales necesitan capacitarse, mantenerse actualizados y adquirir conocimientos en los sistemas tecnológicos de IA para proteger derechos fundamentales como la protección a la privacidad, transparencia y no discriminación. En este marco, la justicia ahora se encuentra en manos de la IA, siendo crucial evaluar adecuadamente las leyes y la aplicación de la ética en los sistemas jurídicos (Farfán Intriago, 2023).

La implementación de la inteligencia artificial en el derecho tiene varias ventajas, así como también, ofrece oportunidades que van a ser de gran ayuda en los procesos judiciales. Además, es una fuente de apoyo para los profesionales del derecho, al momento de realizar sus actividades laborales, puesto que, serán más eficiencia y de mejor efectividad en la prestación de servicios legales.

Los expertos en el derecho tendrán tres beneficios que pretenden ser de gran ayuda para mejorar la justicia. En primer lugar, se podrán utilizar sistemas basados en IA a fin de automatizar tareas que son rutinarias y repetitivas de manera rápida y efectiva, esto con el propósito de optimizar tiempo y que los expertos en el derecho puedan enfocarse en otras tareas más estratégicas y complejas para obtener resultados positivos en la práctica (Farfán Intriago, 2023).

En segundo lugar, los sistemas de IA podrán ayudar a resolver conflictos y tomar decisiones por medio de algoritmos que exploren la base de datos informáticos legales de casos anteriores para resolverlos con mayor precisión y aplicarlos para casos futuros. Por último, los sistemas de IA protegerán el derecho a la igualdad y no discriminación por medio de la disminución de sesgos en el proceso judicial, garantizando el trato justo ante la ley para todas las personas (Caló, 2017).

Sin embargo, también se pueden presentar riesgos al momento de utilizar sistemas de IA en los procesos judiciales. Como es el caso de existir desconfianza de implementar sistemas con IA, puesto que, aún no se ha verificado que tan confiables pueden llegar a ser. Al igual, los sistemas de IA no son claros, por lo que, podría afectar el principio de la motivación al momento de la toma de decisiones.

Por último, la implementación de máquinas inteligentes podría generar pérdida de empleos y disminución de oportunidades laborales por las distantes funciones que brinda la misma. No obstante, no se debe permitir que se reemplace a los profesionales del derecho como jueces y abogados por sistemas expertos jurídicos, debido a que se estaría afectado al proceso judicial y deshumanizando la justicia que es creada para las personas.

La utilización de la IA en el derecho tiene ventajas como desventajas, aunque la Unión Europea establece grandes retos que van a generar controversias en el ámbito jurídico que más adelante se analizarán a mayor profundidad. No obstante, es importante abordar este tema debido a que, esto definirá el mundo en el que vamos a vivir, puesto que la justicia se encuentra en juego, convirtiéndose en una lucha con la tecnología.

Inteligencia artificial en el ámbito penal

La Unión Europea, en la resolución del parlamento, establece que el sistema de IA debe ser utilizado para asuntos penales por agentes oficiales, jueces y demás profesionales, puesto que esto va a significar un aporte fundamental en el derecho penal. Se trata de un sistema de IA con el objetivo de calcular las probabilidades que tiene una persona en cometer un ilícito, más bien tener una predicción criminal, para evitar que se consume el delito (Comisión Europea, 2020).

En este marco, el parlamento europeo desea implementar dos sistemas para la utilización de la IA como es el policing y el sentencing. Esto hace alusión a los sistemas con inteligencia artificial policial (IAP) que sirven para prevenir el cometimiento de delitos y ayudar en la investigación policial para la delincuencia. Asimismo, sistemas con inteligencia artificial judicial (IAJ) para aplicarlo en cada una de sus fases y etapas, a fin de encontrar al culpable del cometimiento de un delito; es decir, se aplicará en la persecución criminal, la investigación delictual y en el juzgamiento para atribuir la responsabilidad por el cometimiento de un delito (Miró Llinares, 2018).

Estos sistemas serán empleados en los procesos penales, específicamente en el área de información e investigación, a fin de prevenir que se consume un delito. No obstante, la implementación de estos sistemas en el proceso penal introduce retos y desafíos como sesgos y discriminaciones en la toma de decisiones legales y demás casos que vulneran derechos fundamentales y quebrantan la justicia.

Bart Verheij (2020), establece tres formas para disminuir los riesgos en los procesos penales. Se resume a tres desafíos, estos son: Primero que la IA debe ser para todas las personas, segundo la IA al momento de tomar decisiones independientes, estas deben ser motivadas, de manera que sea transparente y proporcione explicaciones justificadas; y, por último, la IA debe seguir las reglas establecidas en los diferentes cuerpos normativos, para garantizar el uso responsable.

En este contexto, se cuestiona quién, será el responsable por los delitos ocasionados por IA, hasta el momento no se tienen respuestas para esta interrogante, por ende, es necesario realizar un estudio sobre el status procesal de los sistemas de IA e implementar normativa para este acontecimiento, puesto que, toda innovación requiere el planteamiento de nuevos desafíos legales. A continuación, los principales problemas que se presentan en el sistema jurídico por el uso de la tecnología con IA son alarmantes, por esta razón es necesario analizar tres casos que van a ser de ayuda para comprender que la tecnología es el motor de la sociedad y de tal manera puede lesionar derechos fundamentales.

Todo esto será de mejor entendimiento por medio del análisis de tres casos prácticos. Estos son: Un vehículo autónomo que atropella a una persona, dando como resultado la muerte. El uso de bots para influir en resultados de procesos electorales. Utilización de sistema con IA para fines ilícitos. Se analizarán cada uno de los casos prácticos:

Como primer caso se tiene a un vehículo autónomo que atropella a una persona, con resultado de muerte. La industria automotriz ha dado paso a una revolución en la movilidad mediante sistemas con IA que cuentan con sensores más precisos para reducir los accidentes de tránsito y mejorar la seguridad vial. Sin embargo, el problema surge respecto a la responsabilidad de los conductores de vehículos autónomos cuando se ocasione un accidente. Por mejor decir, ¿A quién se le atribuye responsabilidad cuando un vehículo autónomo esté manejando? ¿De quién será la responsabilidad penal en este caso? Con base a esto surge otra interrogante ¿Nuestra normativa es apta para resolver estos conflictos? (Velazquez Palmero, 2023).

Tal es el caso de un accidente automovilístico que sucedió el 19 de marzo de 2018 en Arizona, Estados Unidos. En donde una compañía de vehículos sin conductor operado por Uber se encontraba realizando pruebas de manejo, atropelló a una mujer de 49 años que se encontraba cruzando fuera del paso peatonal, dando como resultado la muerte. A partir de ese lamentable accidente se suspendieron las pruebas de vehículos sin conductor (Canó, 2018)

En este marco, la persona que conduce un vehículo y ocasiona un accidente será el responsable; sin embargo, en un vehículo autónomo surge la controversia de quién, será el responsable. Se presume que la tecnología es perfecta y está diseñada para prevenir y evitar cualquier accidente. No obstante, en caso de producirse un accidente, el responsable sería el fabricante de ese vehículo debido a que fue consecuencia de un defecto del sistema automotriz el que ocasionó el accidente, por lo que, ese vehículo es defectuoso (Idoia Salazar, 2020).

Bajo este mismo marco, se desplazan dos supuestos básicos para saber a quién se le va a atribuir responsabilidades penales, si bien será responsable el fabricante del vehículo autónomo por algún defecto que ocasionará la pérdida de sus sensores para evitar o prevenir cualquier siniestro o la responsabilidad de la administración pública por defectos en la infraestructura vial.

Además, no se debe descartar el hecho que la persona haya cruzado fuera del paso peatonal, se entiende que el peatón estaba excediendo el riesgo permitido, puesto que, circulaba dentro de las vías y no en paso peatonal, colocándose en una posición de auto puesta en peligro, esto quiere decir que está asumiendo el riesgo. Sin olvidar que no se está respetando el reglamento de tránsito de peatones en cuanto a las obligaciones que deben cumplir como es; circular fuera de vía y cruzar por pasos peatonales.

En este contexto, si se produce accidentes automotores, que el autor sea un vehículo autónomo, se asumirá que es un defecto o problema de la infraestructura vial, puesto que, se justifica que la tecnología es perfecta y los vehículos van a estar diseñados para detectar, prever o evitar un resultado lesivo y de no ser así, será responsable penalmente la persona que lo diseñó por tener un sistema defectuoso.

Como se puede observar, es necesario elaborar nuevas reglas y procedimientos para determinar la responsabilidad en casos de accidentes de vehículos autónomos. Así como normativo para el fabricante del vehículo y con relación al desarrollo del sistema de software. Es decir, el ordenamiento jurídico se debe acoger a la teoría de la responsabilidad ya mencionada, que es la del producto defectuoso y la responsabilidad del fabricante en virtud de que ambas suposiciones van a ocasionar daños (Parlamento Europeo, 2017).

Ahora bien, se encuentra comprobado el impacto que tiene la IA en el derecho, evidenciando la estrecha relación con el mismo. Los regímenes jurídicos relativos a la responsabilidad, el Parlamento Europeo advierte que ahora en adelante todo sistema va a gozar de inteligencia teniendo la capacidad de aprender y tomar decisiones independientes, por lo que, es crucial revisar el régimen jurídico sobre la responsabilidad para poder responder de manera clara estos problemas que implican a las máquinas dotadas de IA.

El segundo caso, consiste en el uso de bots para influir en los resultados de procesos electorales. El uso de las redes sociales se ha convertido en una herramienta clave para comunicarnos e informarnos, dejando a un lado la comunicación tradicional. La influencia que tienen las redes sociales en la actualidad es significativa, tal es el caso de la elección presidencial de Estados Unidos en el año 2016, cuando Donald Trump utilizó bots sociales, que son algoritmos informáticos automatizados, en la red social Twitter, que consistía en crear seguidores con nombres falsos para tuitear a favor del candidato (PortalTIC, 2018).

La estrategia del candidato, era utilizar bots en Twitter para difundir información verdadera o falsa e influir en las personas, especialmente en las que tenían ideales afines poniendo en peligro a la democracia. No es novedoso que los políticos busquen la manera de manipular la opinión pública, más bien lo alarmante es que, la utilización de bots y redes sociales generan una crisis social, vulnerando derechos fundamentales como la libertad de elegir y ser elegido, así como también la libertad de expresarse.

Las redes sociales distorsionan la información, por ende, también la legitimidad de la participación de los candidatos, poniendo en peligro la democracia. A continuación, se analizará un caso para reflexionar sobre la importancia de difundir información y la influencia que tiene en las campañas electorales.

El estadillo social chileno que ocurrió el 18 de octubre de 2019, en donde se empezó a difundir información por medio de bots y las redes sociales sobre los graves incidentes que estaban ocurriendo en el país, generando una crisis social. El Ministerio del Interior el 19 de diciembre de 2019 entregó al Ministerio Público un informe de 112 páginas que abarcaba en resumen el comportamiento de las redes sociales durante el conflicto social (Ayala C, 2019).

El Ministro del Interior a través del análisis big data identificó que existía información delicada con los suficientes antecedentes para iniciar una investigación penal, el informe incluía el incendio de autobuses, edificios, hoteles, iglesias, saqueos a supermercados y locales comerciales, la destrucción de 78 estaciones de metro. Además, analizaron sesenta millones de comentarios publicados en la red social Twitter de cinco millones usuarios. Sin embargo, identificaron que más de once mil usuarios eran bots, cuentas creadas desde que se inició las manifestaciones sociales.

El Fiscal se pronunció respecto a estos acontecimientos, manifestando que es un informe basado en redes sociales, prensa nacional y extranjera, como también de fuentes abiertas, por lo que, deja sin valor la información que contenía, puesto que, no tenían las suficientes pruebas para demostrar que son verdaderos (Díaz Montero, 2020).

El último caso hace referencia a la utilización de sistemas con IA para fines ilícitos, denominado como ciberdelincuencia. Estos delitos son catalogados como ciberdelitos, en donde se encuentran las siguientes figuras delictivas como el robo de identidad, delito informático, acoso, falsificaciones y la estafa (Pons Gamón, 2017). En estos sistemas con IA se desprenden los siguientes tipos de amenazas que están relacionados con la ciberdelincuencia.

La estafa informática es un ciberdelito que consiste en inducir al engaño a una persona mediante correos electrónicos que ofrezcan dinero a cambio de un ingreso por adelantado, perjudicando, de este modo, el patrimonio de la víctima. En esta figura delictiva se desprenden dos tipos de delitos asociados con la IA, el phishing y carding.

El phishing es un ciberataque informático que comúnmente se configura en empresas o bancos, con la finalidad de conseguir datos privados de usuarios o empresa y cometer delitos informáticos. Esta figura delictiva consiste en enviar correos o enlaces maliciosamente a terceras personas, como empleados o clientes, para inducirles al engaño y adquirir un conjunto de datos personales, de forma que puedan hacerse pasar por ellos. Esto con el objetivo de cometer ilícitos como robo de dinero por medio de la obtención de contraseñas bancarias, transferencia de dinero a otras cuentas, así como también, realizar cargos fraudulentos de tarjetas de crédito.

Un ejemplo claro sobre estos sistemas informáticos que afectan el patrimonio de las personas es conocido como fraude del CEO. Estos ciberdelitos surgen generalmente en los bancos en donde se hacen pasar por empleados de una empresa con la capacidad de acceder a cuentas financieras para realizar transacciones a otras cuentas. Sin embargo, por medio de correos electrónicos engañan a los empleados de la empresa para que realicen depósitos urgentes debido a una operación crítica que está atravesando la organización (Banco Pichincha, 2021).

En este caso, el sistema jurídico ha determinado que la responsabilidad va a ser del banco, es decir, de quien provee los servicios de pago, salvo que se demuestre que es fraude o negligencia por parte de la víctima. Sin embargo, también se puede prevenir por medio de sistemas de seguridad para reconocer que los correos o enlaces no son auténticos. Por otro lado, el carding, consiste en copiar los dígitos de las tarjetas de crédito para ser utilizada posteriormente de acuerdo con sus intereses, al igual que el phishing, también se puede prevenir por medio de, ciberseguridad.

Los delitos informáticos de daños, conocidos también como virus informáticos, son utilizados para borrar, dañar, alterar informaciones o suprimir datos informáticos. En cambio, los sistemas que son utilizados en contra de la voluntad de las personas, para adquirir su información personal, es conocido como delitos a la intimidad. Por último, los drones se han convertido en una nueva herramienta para cometer ilícitos. Los cibercriminales la están utilizando para vigilar y espiar las residencias de cualquier persona, adquiriendo información favorable para sus atracos. Por ejemplo, saber a qué hora la casa se encuentra vacía, a qué hora llegan, si existe algún mecanismo de seguridad, entre otros.

Estos son los casos en donde la IA ha generado problemas en el tráfico jurídico. Por lo que, la forma en la que se resuelvan va a significar un precedente significativo para el derecho penal. Siendo un reto, para los sistemas con IA sean creados y utilizados con transparencia, responsabilidad, así como también con principios éticos.

Además, los sistemas de IA que gozan de autonomía deberán ser responsables penalmente por sus actos ilícitos. En este sentido, con el análisis de estos casos podemos dar respuesta a varias inquietudes, para lo cual se debe considerar lo siguiente: 1) los sistemas de IA están siendo utilizados como un medio para la comisión de un delito, siendo responsable únicamente la persona que voluntariamente utilizó sistemas de forma indebida para cometer un acto delictuoso; y, 2) será responsable la persona que pudiendo abstenerse de realizar esa conducta con resultado lesivo, no lo hizo y programó el sistema de IA para cometer un delito.

Por lo tanto, la utilización de sistemas con IA en el ámbito penal conlleva una serie de riesgos, puesto que, la mayoría son utilizados para fines delictivos. Además, se tendrá un comportamiento perjudicial que amenaza a la humanidad. En este sentido, la IA tienen cuatro desafíos importantes que se presentan en el derecho penal. Estos son: el uso de la IA deberá ser ética, la IA debe ser social; es decir, con la interacción de los humanos sin discriminación, la IA deberá ser explicable, para garantizar la transparencia al proporcionar explicaciones justificadas; y, la IA debe ser responsable, guiarse por las reglas, normas y leyes de la sociedad.

Antes se pensaba que los dilemas éticos en los sistemas de IA desde la perspectiva jurídica no era un problema, puesto que, se manifestaba que la tecnología era incapaz de crear máquina que tenga coincidencia y autonomía. Por lo que, la ética sería neutra, con el paso del tiempo la tecnología se convirtió en el motor del mundo, elaborando sistemas capaces de tener autonomía generando un impacto que causados estragos en el derecho y es controversial (Parra Sepúlveda, 2021).

Por esta razón, el desafío ético va encaminado en controlar que las personas no utilicen los sistemas de IA de forma maliciosa. Dando a entender que la identificación de principios, valores y la ética en la IA es la base para una sociedad responsable, juntamente con la implementación de políticas públicas y privadas que regulen a la tecnología.

El Parlamento Europeo (2020), en su propuesta de legislación sobre el uso de sistemas con IA, robótica y tecnologías asociadas, reconoce e identifica los principios éticos que deben ser considerados en el marco jurídico para regular a la IA. En el artículo 4 en su parte pertinente, manifiesta que toda IA, robótica y tecnologías relacionadas, se deberán desarrollar y utilizar de conformidad con principios éticos. El desarrollo y uso de la IA se llevarán a cabo para garantizar la dignidad humana y los derechos fundamentales de las personas; así como también se llevarán a cabo para mejorar los intereses de los ciudadanos, protegiendo y fomentando el bienestar social (European Parliament, 2020).

En cambio, al hablar de IA con interacción social sin discriminación, hace referencia que el derecho debe garantizar a todas las personas el acceso a los sistemas de IA. De la misma manera, los sistemas de IA para garantizar la transparencia al proporcionar decisiones deberán ser justificados, conforme a las leyes que rigen en cada materia. Además, deben ser explicados con un lenguaje claro y comprensible para todos los seres humanos. Los sistemas de IA tienen como finalidad resolver conflictos y utilizar tecnología basada en IA en los juzgados para agilizar, tomar decisiones rápidas, maximizar trámites y minimizar costos procesales.

Por último, el sistema de IA debe ser responsable; cumpliendo con reglas, normas y leyes con el propósito de prevenir que se utilicen para fines delictivos. Sin embargo, se implementará normativa para establecer responsabilidad penal y cuando se configure un delito en donde se encuentre implicada, la inteligencia artificial tendrá su respectiva sanción.

Propuesta de normativa para regular a la IA

El derecho surge con las necesidades de la sociedad. Por lo que, es necesario implementar normativa con base a los desafíos y retos que la IA ofrece. Así como también aprovechar las oportunidades que tiene la misma. Haciendo esta reflexión, la propuesta de normativa debe regular las actividades relativas a la IA, enfocado en el ser humano, con el objetivo de fomentar la innovación, potenciar la utilización de tecnología y reforzar la protección de datos por medio de ciberseguridad para tener sistemas con IA de confianza. Además, establecer un marco ético y legal de la IA y un marco de responsabilidad para los proveedores de IA (Martínez Espín, 2023).

En este sentido, el desarrollo de una legislación apropiada para el diseño y uso responsable de sistemas con IA debe integrar los siguientes principios. La inclusión, responsabilidad, transparencia y justicia, que además sirven de nexo entre lo ético y jurídico, al igual establecer normas especiales de naturaleza sectorial para garantizar el desarrollo confiable de la IA con base, al campo que desempeñe y responder a las problemáticas sobre el régimen de responsabilidad y la protección de datos personales.

El objetivo de la propuesta es prohibir la utilización de sistemas con IA que puedan poner en peligro la seguridad de las personas, así como también vulnerar derechos fundamentales. Los creadores de sistemas con IA deben ser transparentes, brindar toda la información, de forma clara y comprensible, sobre el funcionamiento y sus limitaciones. Además, impulsar mecanismo de gobernanza que se centre en la actividad humana, la supervisión o control de los sistemas con IA por personas capacitadas (Martínez Espín, 2023).

La regulación de la IA debe respetar los derechos fundamentales para garantizar el bienestar de las personas y de la sociedad, puesto que, se están creando programas con discriminación algorítmica un ejemplo de ello el programa de riesgos COMPAS utilizado por jueces de EE. UU para determinar la tasa de reincidencias, en donde se comprobó que para personas negras tienen una tasa más elevada que personas blancas, dejando en claro la vulneración al derecho de igualdad y no discriminación (Parra Sepúlveda, 2021).

Con base a esto, es necesario que los sistemas con IA se sometan a un proceso de certificación antes de ser utilizados y que sean supervisados o controlados por personas capacitadas, quienes serán los responsables de garantizar el cumplimiento de las normas establecidas y controlar el funcionamiento de los sistemas.

En este marco, la propuesta de regulación de la IA se centra en los siguientes aspectos importantes para proteger los derechos fundamentales de las personas. Primero, se deben prohibir ciertas prácticas de acuerdo con su grado de peligrosidad, los sistemas con un riesgo inaceptable se encuentran prohibidas, puesto que, pueden manipular el comportamiento humano como vigilancia masiva, difundir información falsa y demás delitos. Segundo, los proveedores y los usuarios de sistemas con IA deben tener obligaciones para garantizar la seguridad y protección de datos, así como también, que su utilización sea transparente, responsable por medio de evaluaciones de riesgo y mantenimientos (Martínez Espín, 2023).

Tercero, los sistemas de alto riesgo deben someterse a un proceso de certificación antes de ser utilizados bajo la supervisión de personas capacitadas, quienes serán los responsables de garantizar el cumplimiento de las normas establecidas y controlar el funcionamiento del sistema. Por último, fomentar la cooperación internacional para desarrollar normas globales, en colaboración con organizaciones internacionales. Así como la propuesta de la Comisión Europea que establece alianzas internacionales para adoptar prácticas éticas y responsables.

En este sentido, se debe regular a la IA en los siguientes parámetros específicos en la protección de datos por medio de una evaluación y medidas técnicas para detectar riesgos y posibles afectaciones al sistema, así mismo, una regulación en la justicia para garantizar la transparencia en la toma de decisiones y proteger derechos fundamentales. Regulación para vehículos autónomos con la finalidad de garantizar la seguridad vehicular. En cuanto, a la regulación de seguridad, se debe implementar normas para garantizar la privacidad en los sistemas utilizados para vigilancia y seguridad pública.

De la misma manera, se necesita implementar normativa para proteger al consumidor, es decir, atribuyendo ciertas obligaciones y responsabilidades al proveedor en relación con la comercialización de sistemas inteligentes para evitar que se vulneren derechos y sean utilizadas de forma

ilícita. Por lo que, debe garantizar la seguridad y fiabilidad de sus productos. Además, ofrecer información clara sobre el funcionamiento, capacidades y limitaciones. Por otro lado, para medir y conectar ese compromiso previo a la instalación se le va a otorgar un identificador único y anónimo ID al consumidor para asegurar que no sea utilizado para fines delictivos.

Es importante que los proveedores cuenten con un seguro de responsabilidad para cubrir con los posibles daños en caso de estar defectuoso o presente algún daño al sistema con IA, puesto que si se puede pedir una indemnización al proveedor sin la necesidad de demostrar la culpa del fabricante. Esto se hace con la intención, que los creadores diseñen sistemas seguros, con los permisos para su comercialización, por lo que, los responsables no solo son los fabricantes sino también los proveedores porque están influyendo en el funcionamiento del producto.

Metodología

La investigación se llevó a cabo bajo un enfoque cualitativo, que incluyó una exhaustiva revisión bibliográfica, análisis doctrinal, evaluación de criterios y opiniones de diversos tratadistas y profesionales del derecho. Además, se recopiló información de bases de datos y otras fuentes relevantes para fundamentar teóricamente el papel de la inteligencia artificial en el derecho penal. El nivel de profundidad de la investigación se caracterizó como descriptivo-explicativo, considerando los problemas y desafíos que representan una amenaza para el ordenamiento jurídico.

Para abordar la problemática, se aplicaron diversos métodos. Se utilizó el método deductivo-inductivo para realizar un análisis general sobre la inteligencia artificial, desde su origen hasta las implicaciones en el ámbito penal, permitiendo así comprender la problemática y explicarla a partir de teorías relacionadas con la inteligencia artificial. Asimismo, se empleó el método analítico-sintético para examinar casos específicos en los que la inteligencia artificial estuvo involucrada en la comisión de delitos, lo que facilitó el análisis de las implicaciones procesales y penales de dichas conductas ilícitas. Finalmente, se recurrió al método dogmático-jurídico para estudiar el derecho penal en relación con la inteligencia artificial, identificando la falta de normativa específica y proponiendo una legislación para regular el uso de la inteligencia artificial en el ámbito jurídico.

Entre las técnicas utilizadas, se destacan las entrevistas realizadas a profesionales del derecho, con el objetivo de recabar sus opiniones y criterios sobre la aplicación de la inteligencia artificial en el derecho penal, así como sobre la responsabilidad penal de las personas en el contexto de la inteligencia artificial. Además, se desarrollaron guías para la realización de estas entrevistas, que sirvieron como instrumentos para recopilar información relevante y detallada de los expertos en la materia.

Resultados

Se llevaron a cabo entrevistas con profesionales del derecho con el propósito de obtener una comprensión detallada de su perspectiva sobre la aplicación de la inteligencia artificial en el ámbito del derecho penal. Con este fin, se desarrolló una tabla para organizar las diversas opiniones recopiladas durante las entrevistas. Además, se condujo una entrevista semiestructurada que incluyó tanto preguntas abiertas para explorar la visión general de los expertos sobre el tema de investigación, como preguntas cerradas para obtener información específica sobre sus opiniones. Estas entrevistas fueron realizadas a tres abogados en ejercicio independiente, un juez y un fiscal. Los resultados obtenidos fueron los siguientes:

Tabla 1. Resultados de las entrevistas.

| Preguntas | Abogado 1 | Abogado 2 | Abogado 3 | Juez | Fiscal |
|--|--|--|---|---|--|
| ¿Existen riesgos éticos con el uso de sistemas con IA en la toma de decisiones judiciales? | Si existen, riesgos éticos porque se puede afectar el principio de la motivación | El uso de sistemas con IA puede vulnerar principios y derechos como el de igualdad y no discriminación | La ética en el derecho es fundamental por lo que sí afecta a las decisiones judiciales. | Las decisiones judiciales deben ser motivadas por lo que la utilización de la IA puede afectar la transparencia en la toma de decisiones. | Utilizar la IA en el derecho presenta beneficios como riesgos y uno de ellos es la ética en la toma de decisiones. |
| ¿Cuáles son los desafíos legales que se presentan en el derecho penal por la utilización de la IA? | El desafío de tener seguridad y protección de datos personas | Actualizarse para manejar a la IA, puesto que el desconocimiento genera incertidumbre y desconfianza | La desconfianza en implementar IA en el derecho | Los sistemas con IA deberían ser sometidos a rigurosas pruebas para lograr su aceptación en el derecho. | Va a existir conflicto de normativa. |
| ¿Considera que la IA es un beneficio para derecho? | Si porque se puede optimizar tiempo | Permite mejorar la calidad de servicios legales | Nos ayudar a resolver casos de manera más rápida y efectiva | Si porque, se tiene como garantía la imparcialidad en la toma de decisiones | Nos permite acceder de forma más rápida a la base de datos y permite mantener los procesos más sistematizados y ordenados. |
| ¿Cree que necesitamos normativa específica para el uso de sistemas con IA? | Es fundamental la creación de normativa para evitar conflicto de leyes | Se necesita de una normativa para que sea más seguro la utilización de la IA | Es necesario implementar normativa para prevenir la vulneración de derechos | Si necesitamos de normativa para que los posibles conflictos se resuelvan con base a derecho | Se necesita de normativa para atribuir responsabilidad penal en caso de ser utilizado para fines ilícitos |

Fuente: Entrevistas. Elaboración propia.

Con base, a las entrevistas realizadas a los expertos en el derecho se ha demostrado que la mayoría concuerda que es un desafío para el derecho la implementación de la IA como un método que garantice la ética, transparencia y responsabilidad en la toma de decisiones judiciales debido a que, deben ser motivadas. Sin embargo, los dilemas éticos y transparencia en el derecho más bien están enfocados a que las personas los utilicen con responsabilidad poniendo en juego sus valores y sobre todo su transparencia para evitar injusticias al no fortalecer a los fines ilícitos, por lo que es necesario establecer los límites para evitar conflictos.

Además, concuerdan que los sistemas con IA traen consigo problemas y desafíos al momento de utilizar algoritmos en los procesos judiciales, tales como, la desconfianza de implementar IA, puesto que, aún no se ha verificado que tan confiable puede llegar a ser. Al igual que, los sistemas de IA no son claros, por lo que, podría afectar el principio de la motivación al momento de tomar decisiones.

Las personas tenemos miedo a lo desconocido, es por ello que la información y el conocimiento nos permitirá adentrarnos en la nueva era tecnológica que estamos atravesando, y esto obliga a que los profesionales del derecho y de todas las ramas se mantengan actualizando sus conocimientos, estudiando las nuevas tecnologías que surgen día a día, porque sería inaceptable darle la espalda al futuro. Conocer y adentrarse al magnífico mundo de la IA, nos permitirá determinar qué herramientas usar en nuestro ejercicio profesional y seleccionar el algoritmo ideal que se ajuste a nuestras necesidades; incrementando significativamente la eficiencia en los procesos judiciales.

Los beneficios para los profesionales del derecho en utilizar sistemas inteligentes para automatizar tareas que son rutinarias y repetitivas de manera rápida y efectiva, esto con el propósito de optimizar tiempo. Así mismo, ayudan a resolver conflictos y tomar decisiones por medio de algoritmos que exploren la base de datos informáticos legales de casos anteriores para resolverlos.

Por último y más importante, los expertos en el derecho han manifestado que es necesario implementar normativa para regular a la IA en el derecho y evitar conflictos de leyes o vacíos legales. Lo cual requiere crear una regulación que garantice el uso responsable sin frenar el progreso. Además, establecer responsabilidad penal para cuando se configure un delito en donde se encuentre implicada la inteligencia artificial, tendrá su respectiva sanción.

Discusión

La propuesta de regulación de sistemas con IA se centra en cuatro dimensiones para proteger los derechos fundamentales. Primero, debe contener principios y reglas básicas del derecho, así como también prohibir ciertas prácticas de acuerdo con su grado de peligrosidad, puesto que, pueden manipular el comportamiento humano como vigilancia masiva, difundir información falsa y demás delitos. Segundo, los proveedores y los usuarios de sistemas con IA deben tener obligaciones para garantizar la seguridad y protección de datos, así como también, que su utilización sea transparente, responsable por medio de evaluaciones de riesgo y mantenimientos. Tercero la supervisión o control de los sistemas con inteligencia artificial deben ser competencia de las personas y, por último, no debe entorpecer la innovación de la inteligencia artificial, puesto que, a través de reglas efectivas de responsabilidad va a seguir progresando y siendo de apoyo para los profesionales del derecho.

Conclusión

El surgimiento de la inteligencia artificial en el derecho ha ocasionado cambios significativos en cada una de sus ramas trayendo consigo desafíos, problemas y oportunidad. Desafíos, como la desconfianza de implementar sistemas con IA puesto que, aun no se ha verificado que tan confiables pueden ser. Al igual, los sistemas con IA podrían afectar el principio de la motivación al momento de tomar decisiones.

Los beneficios que ofrece la IA son diversos para las profesiones del derecho, como automatizar y sistematizar tareas de manera rápida y efectiva, esto con el propósito de optimizar tiempo. Además, ayudan a resolver conflictos y tomar decisiones con mayor precisión para aplicarlos en casos futuros. Así mismo, protege el derecho a la igualdad y no discriminación, garantizando el trato justo ante la ley para todas las personas.

Los problemas que se presenta en el ámbito penal por la utilización de sistemas con IA conllevan una serie de riesgos, puesto que, la mayoría, son utilizados para fines delictivos. Con base, a los tres casos prácticos se ha determinado lo siguiente: Los sistemas de IA están siendo utilizados como un medio para la comisión de un delito, siendo responsable únicamente la persona que voluntariamente utilizó sistemas de forma indebida para cometer un acto delictuoso; y será responsable la persona que pudiendo abstenerse de realizar esa conducta con resultado lesivo, no lo hizo y programó el sistema de IA para cometer un delito.

Además, el uso de sistemas con IA, deberá ser ética, social, con la interacción de los humanos sin discriminación, ser explicable, para garantizar la transparencia al proporcionar explicaciones justificadas, y la IA debe ser responsable; es decir, guiarse por las reglas, normas y leyes de la sociedad.

Es indispensable crear normativas para cualquier elemento que se introduzca a la sociedad, sobre todo cuando se pretende su buen uso para beneficio y progreso de la humanidad. Con base a lo antes mencionado, no se puede realizar una normativa de manera precipitada sino más bien, debe desarrollarse paralelamente conforme avanza la tecnología, tomando la inteligencia artificial como una herramienta a favor del derecho, y no como una fuente que reemplace a las personas, debido a que las leyes se hicieron para proteger a las personas, mas no a la tecnología, quitando la esencia del derecho y deshumanizando la justicia.

Referencias

- Araya Paz, Carlos. (2020). Desafíos legales de la inteligencia artificial en Chile. *Revista chilena de derecho y tecnología*, 9(2), 257-290. <https://dx.doi.org/10.5354/0719-2584.2020.54489>
- Ayala, C.L. (2019, 21 de diciembre). El big data del Gobierno: Los detalles del informe por el estallido social que entregó a la Fiscalía. *LT La tercera*. <https://acortar.link/2D5mqg>
- Banco Pichincha. (2021, 14 de diciembre). *El fraude del CEO, una estafa que pone en jaque a tu negocio*. <https://www.pichincha.com/blog/que-es-fraude-del-ceo>
- Calo, R. (2017, 19 de octubre). Política de inteligencia artificial: introducción y hoja de ruta. *SSRN*. <https://dx.doi.org/10.2139/ssrn.3015350>
- Canó, R.J. (2018, 20 de marzo). Primer atropello mortal de un coche sin conductor. *El Pais*. https://elpais.com/tecnologia/2018/03/19/actualidad/1521479089_032894.html
- Castro Castro, R. J., Chiquito Muñiz, J. J., Romero Castro, M. I., & Clavel Quintero, Y. (2022). La inteligencia artificial y sus diferencias con los sistemas expertos. *Journal TechInnovation*, 1(2), 88–96. <https://doi.org/10.47230/Journal.TechInnovation.v1.n2.2022.88-96>
- Comisión Europea. (2020, 19 de febrero). *LIBRO BLANCO sobre la inteligencia artificial–un enfoque europeo orientado a la excelencia y la confianza*. <https://acortar.link/dYC6mW>
- Comisión Europea. (2018, 25 de abril). *EUR-Lex*. <https://eur-lex.europa.eu/legal-content/ES/TX-?uri=COM%3A2018%3A237%3AFIN>
- Díaz Montero, F. (2020, 15 de enero). “No hemos encontrado ningún valor”: Fiscal Abbott desecha informe Big Data entregado por La Moneda. *Biobiochile*. <https://acortar.link/HRQACM>
- Elizalde Salazar, I. (2020). Capítulo 1. Vehículos autónomos. Desplazamiento de las reglas de responsabilidad civil del propietario al fabricante. Críticas a la propuesta. El riesgo de la circulación seguirá existiendo. En L. Arismendy Mengual, F. Oyarzún Vargas; M.J. Santos Morón, J.R. Mercader Uguina, y P. del Olmo García (coord.). *Nuevos retos del Derecho de Daños en Iberoamérica* (pp. 841-858). Tirant lo Blanch.
- European Parliament. (2020, 21 de abril). *Draft Report with recommendations to the Commission on a framework of ethical aspects of artificial intelligence, robotics and related technologies. Proposal for a Regulation of the European Parliament on ethical principles for the development, deployment*. https://www.europarl.europa.eu/doceo/document/A-9-2020-0186_EN.html
- Farfán Intriago, J.L. (2023). Inteligencia artificial y Derecho: ¿La justicia en manos de la IA? *Frónesis*, 8-13.
- Frosini, V. (2019). *Cibernética, derecho, internet y sociedad*. Olejnik.

- Martínez Espín, P. (2023). La propuesta de marco regulador de los sistemas de Inteligencia Artificial en el mercado de la UE. *Revista CESCO De Derecho De Consumo*, (46), 1–20. https://doi.org/10.18239/RCDC_2023.46.3322
- Miró Llinares, F. (2020). INTELIGENCIA ARTIFICIAL Y JUSTICIA PENAL: MÁS ALLÁ DE LOS RESULTADOS LESIVOS CAUSADOS POR ROBOTS. *Revista de Derecho Penal y Criminología*, (20), 87–130. <https://doi.org/10.5944/rdpc.20.2018.26446>
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura. (2020, 7 de Septiembre). *UNESDOC*. https://unesdoc.unesco.org/ark:/48223/pf0000373434_spa
- Parlamento Europeo. (2017, 16 de febrero). *Resolución del Parlamento Europeo, con recomendaciones destinadas a la Comisión sobre normas de Derecho civil sobre robótica (2015/2103(INL))*. https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_ES.html
- Parra Sepúlveda, D., & Concha Machuca, R. (2021). Inteligencia artificial y derecho. Problemas, desafíos y oportunidades. *Vniversitas*, 70, 1–25. <https://doi.org/10.11144/Javeriana.vj70.iadp>
- Pons Gamon, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad/ Internet, the new age of crime: cybercrime, cyberterrorism, legislation and cybersecurity. *URVIO. Revista Latinoamericana De Estudios De Seguridad*, (20), 80–93. <https://doi.org/10.17141/urvio.20.2017.2563>
- Porcelli, A. M. (2020). La Inteligencia Artificial y la Robótica: sus dilemas sociales, éticos y jurídicos. *Derecho Global. Estudios Sobre Derecho Y Justicia*, 6(16), 49–105. <https://doi.org/10.32870/dgedj.v6i16.286>
- PortalTIC. (2018, 22 de mayo). *Europa Press PortalTIC*. <https://acortar.link/H8wkjf>
- Solar Cayón, J.I. (2020). La inteligencia artificial jurídica: nuevas herramientas y perspectivas metodológicas para el jurista. *Revus*, 41. <https://doi.org/10.4000/revus.6547>
- Velazquez Palmero, C. (2023). La responsabilidad de los vehículos autónomos. *EasyLaw*. <https://easylawmagazine.com/2023/07/27/la-responsabilidad-de-los-vehiculos-autonomos/>
- Verheij, B. (2020). Artificial intelligence as law. *ArtifIntell Law*, 28, 181–206. <https://doi.org/10.1007/s10506-020-09266-0>

Autoras

María Paula Ávila Zea. Licenciada en Derecho, con experiencia en la materia, estudiante del Máster en Derecho Penal y Litigación Oral de la Universidad Católica de Cuenca.

Ana Fabiola Zamora Vázquez. Destacada profesora de Derecho penal con una sólida formación académica. Posee un máster y un doctorado en la materia, destacando por sus investigaciones pioneras en el sistema de justicia penal. Su pasión por la enseñanza y su compromiso con la excelencia académica la han convertido en una figura respetada en el ámbito del derecho penal.

Declaración

Conflicto de interés

No tenemos ningún conflicto de interés que declarar.

Financiamiento

Sin ayuda financiera de partes ajenas a este artículo.

Notas

El artículo es original y no ha sido publicado previamente.