Ciencia y Desarrollo. Universidad Alas Peruanas
http://revistas.uap.edu.pe/ojs/index.php/CYD/index

Recibido 5 de noviembre 2025 - Aceptado 15 de diciembre 2025

INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DIGITAL EN LA LEGISLACIÓN DE DELITOS INFORMÁTICOS

ARTIFICIAL INTELLIGENCE AND DIGITAL PROTECTION IN COMPUTER CRIME LEGISLATION

Blanco Alban Jennifer Allibon[1], Moreno Collao Franchezca Mia Selene[2], Pérez Torres Anderson Alexix[3], Quiliano Espejo Luis Sebastian[4], Ramirez Lamas Ricardo Fabian[5], Reyna García Flavia Alejandra[6], Felipa Elvira Muñoz-Ccuro[7]

RESUMEN

El estudio aporta a la meta 9.5 del ODS 9, a promover la innovación, fortalecer la investigación científica en ciberseguridad y mejorar las capacidades tecnológicas para la protección de la estructura digital, estableció como objetivo "analizar cuáles son los principales retos que enfrenta la inteligencia artificial para fortalecer la protección digital según la actual legislación de delitos informáticos, Callao 2024". El método comprendió el enfoque cualitativo; alcance descriptivo; tipo básico; diseño no experimental de teoría fundamentada; técnica análisis documental e Instrumento ficha técnica de análisis documental. El principal hallazgo evidenció que existen vacíos legales ante la sofisticación de ciberdelitos con IA que superan los controles de seguridad actuales. La conclusión refiere la necesidad de modernizar la normativa penal y adoptar defensas tecnológicas avanzadas para proteger los derechos fundamentales.

Palabras clave: Inteligencia artificial; Protección de datos; Legislación; Tecnología; Derecho a la privacidad

ABSTRACT

The study contributes to SDG 9.5, promoting innovation, strengthening scientific research in cybersecurity, and improving technological capabilities for the protection of digital infrastructure. It set out to "analyze the main challenges facing artificial intelligence in strengthening digital protection under current cybercrime legislation, Callao 2024." The method comprised a qualitative approach; descriptive scope; basic type; non-experimental grounded theory design; documentary analysis technique; and documentary analysis technical data sheet instrument. The main finding showed that there are legal loopholes in the face of sophisticated AI cybercrimes that bypass current security controls. The conclusion refers to the need to modernize criminal law and adopt advanced technological defenses to protect fundamental rights.

Keywords: Artificial intelligence; Data protection; Legislation; Technology; Right to privacy

1. Universidad Cesar Vallejo. jblancoal@ucvvirtual.edu.pe https://orcid.org/0000-0001-5011-8902
2. Universidad Cesar Vallejo. frmorenoco@ucvvirtual.edu.pe https://orcid.org/0009-0004-7317-6741
3. Universidad Cesar Vallejo. aperezto97@ucvvirtual.edu.pe https://orcid.org/0009-0009-8313-0700
4. Universidad Cesar Vallejo. lsquiliano@ucvvirtual.edu.pe orcid.org/0009-0002-8880-7388
5. Universidad Cesar Vallejo. riramirezla@ucvvirtual.edu.pe https://orcid.org/0009-0001-7429-561X
6. Universidad Cesar Vallejo. flreynaga@ucvvirtual.edu.pe https://orcid.org/0009-0000-1623-40
7. Universidad César Vallejo. Investigador RENCYT. fmunozc@ucv.edu.pe https://orcid.org/0000-0001-9572-1641

INTRODUCCIÓN

La inteligencia artificial es empleada cada vez con más frecuencia para reconocer amenazas cibernéticas, ya que permite revisar enormes cantidades de datos y detectar posibles ataques antes de que ocurran (Chen et al., 2021). Mientras tanto, las leyes y regulaciones siguen adaptándose para poder responder a estos nuevos retos, sobre todo cuando se trata de proteger la información personal y regular el uso de las tecnologías digitales. En este contexto, la investigación resulta importante porque las herramientas de tecnologías de la información se han convertido en un apoyo esencial para enfrentar los delitos informáticos: permiten reunir, organizar y analizar datos que sirven como base para impulsar nuevas investigaciones (Ling et al., 2023).

El impacto tecnológico y social de la inteligencia artificial en la delincuencia cibernética trae consigo tanto riesgos como oportunidades ya que ofrece recursos más sofisticados que también pueden ser aprovechados por los atacantes, complicando la detección de malware, robos de información o tácticas de manipulación social (Das et al., 2022). Por otro lado, los algoritmos de IA generan preocupaciones sobre la privacidad y la seguridad de los datos, incluso cuando existen normas que intentan proteger a los usuarios.

La tecnología analizada se centra en detectar y prevenir delitos informáticos. Por eso, el estudio se relaciona con la meta 9.5 de los ODS, ya que impulsa la creación de infraestructuras más resilientes y promueve la innovación en ciberseguridad. Esto incluye aumentar la investigación y la inversión en este ámbito, así como incorporar tecnologías como la inteligencia artificial en los marcos legales para lograr una legislación más actual, coherente y preparada ante los nuevos avances. (Gundu et al., 2025).

El uso de la inteligencia artificial requiere marcos regulatorios claros. Organismos internacionales como la ONU ofrecen algunas recomendaciones, tales como implementar normas comunes para la evaluación clínica de aplicaciones de IA de alto riesgo y aumentar la transparencia y la evidencia clínica de los dispositivos médicos basados en IA (Chatinakrob, 2024). Por otro lado, un país que está a la vanguardia es Estados Unidos, el cual es líder mundial en investigación y desarrollo de IA, con fuerte inversión en educación y sector privado (Zahra & Nurmandi, 2021). Este país aporta significativamente mediante la creación de políticas que promueven la innovación responsable, el financiamiento de proyectos públicos y privados enfocados. en la seguridad digital y la elaboración de guías éticas para el uso de algoritmos en sectores como la salud y la defensa. Además, su enfoque descentralizado y específico por sectores en la protección de datos y la ciberseguridad facilita que las normativas se ajusten a los requerimientos de cada sector (Alkaabi et al., 2011).

En el contexto nacional, el progreso tecnológico y la integración de la inteligencia artificial (IA) han generado tanto ventajas como desafíos para el marco legal (Mejía Arbildo, 2023). En años recientes, el país ha experimentado un incremento significativo en delitos informáticos relacionados con la suplantación de identidad, fraudes en línea y la violación de datos personales (Mejía Arbildo, 2023). La implementación de la inteligencia artificial en organizaciones tanto del sector público como privado ha puesto de manifiesto la falta de una normativa clara sobre la protección en el entorno digital, ya que la Ley N. º 29733 sobre Protección de Datos Personales no aborda de manera específica los peligros vinculados al uso de algoritmos automáticos y sistemas inteligentes. De igual modo, el uso de la inteligencia artificial en el entorno cibernético del Perú ha sido también explotado por delincuentes digitales, quienes utilizan sofisticadas herramientas tecnológicas para falsificar identidades o alterar datos (Mejía Arbildo, (2023). La ausencia de un marco normativo claro sobre la responsabilidad civil ante los daños causados por sistemas automatizados evidencia un vacío legal (Mejía Arbildo, (2023). Además, la

falta de lineamientos definidos en torno a la ética y la responsabilidad de la inteligencia artificial produce inseguridad jurídica y una regulación dispersa (Zabala Leal 2024)".

Entre los síntomas más notorios se encuentra el incremento de ocasiones relacionadas con deep fakes, robo de identidad y robos digitales; por lo tanto, los sesgos algorítmicos y la oscuridad de sistemas que dañan la justicia predictiva, generando recelo público y cuestionamientos sobre el ecuánime del sistema judicial (Saavedra et al., 2024). Esta situación problemática surge, en parte, por la velocidad con que progresa la tecnología en comparación con la limitada capacidad del marco normativo para adaptarse, así como la falta de mecanismos institucionales adecuados para supervisar el uso de la IA (Novelli 2024) Además, el entrenamiento de algoritmos con datos sesgados contribuye a prácticas discriminatorias en entornos laborales y judiciales (Castillo-Castro, 2025).

Las consecuencias que genera este hecho vulneran derechos fundamentales como la privacidad, el honor y la identidad digital, mientras que la ausencia de lineamientos sobre responsabilidad civil deja a las víctimas sin garantías jurídicas, generando además pérdidas económicas y reputacionales y debilitando la confianza en el sistema judicial (Zabala & Gómez, 2024; Concha, 2024). Para abordar esta problemática, se requiere fortalecer la legislación penal y civil vinculada a la IA, implementar auditorías de algoritmos y mecanismos de transparencia, y promover políticas de ética digital junto con la capacitación de operadores judiciales, con el fin de reducir la opacidad tecnológica y proteger los derechos fundamentales frente a los delitos informáticos (Saavedra et al., 2024; Castillo-Castro, 2025) .El desafío presente radica en respaldar que el desarrollo tecnológico avance de la mano con la seguridad de los derechos humanos. La formación de protocolos de supervisión, el establecimiento de patrones de seguridad y la promoción de una civilización digital responsable son actos esenciales para reducir los riesgos derivados del uso inadecuado de la inteligencia artificial. Solo por medio de una regulación clara y mecanismos de control eficaces será posible asegurar un entorno digital más seguro, justo y transparente.

En ese marco se formularon los problemas del estudio. Como problema general se planteó: ¿Cuáles son los principales retos que enfrenta la inteligencia artificial para fortalecer la protección digital según la actual legislación de delitos informáticos? A partir de ello, se definieron dos problemas en específicos: Primero, ¿Cómo las nuevas aplicaciones de IA en ciberdelitos requieren de nuevas técnicas de protección y ciberseguridad más efectivas considerando la legislación de delitos informáticos? Y segundo, ¿En qué medida los mecanismos de protección digital y ciberseguridad resultan eficaces frente a las amenazas emergentes asociadas al uso de inteligencia artificial en delitos informáticos? Seguidamente se establecieron los objetivos de estudio. El objetivo general es: Analizar cuáles son los principales retos que enfrenta la inteligencia artificial para fortalecer la protección digital según la actual legislación de delitos informáticos. Mientras que los objetivos específicos. Primero, es analizar cómo las nuevas aplicaciones de IA en ciberdelitos requieren de nuevas técnicas de protección y ciberseguridad más efectivas, considerando la legislación de delitos informáticos.

Y segundo, evaluar la eficacia de los mecanismos de protección digital y ciberseguridad frente a las amenazas emergentes asociadas al uso de inteligencia artificial en delitos informáticos, dentro del marco de la legislación.

Con relación a los antecedentes que sostienen el trabajo de investigación, tenemos a Kavitha & Thejas (2024), que explican la "Teoría de modelos de aprendizaje automático y profundo", donde destacan el uso de modelos tradicionales (SVM, Random Forest) y avanzados (CNN, RNN, GANs), así como enfoques híbridos y de IA explicable, para aumentar la precisión y la

interpretabilidad en la detección de amenazas. Esto se relaciona con IA y protección de datos digital al aportar herramientas técnicas para la detección, prevención y respuesta a delitos cibernéticos. La metodología mixta con enfoque experimental, en el cual se evalúan modelos de aprendizaje profundo, aprendizaje automático, GANs y técnicas híbridas para la protección digital. El principal hallazgo demostró nuevos peligros y resaltó la necesidad de defensas completas en el entorno digital actual. Se muestra cómo la IA puede transformar, tanto en la práctica como en las leyes, la defensa contra los delitos informáticos, haciendo esencial que se deba agregar en las reglas y políticas de seguridad digital.

Siam et al. (2025) explica la "Teoría de sistemas adaptativos y proactivos en ciberseguridad", donde menciona que las soluciones basadas en IA permiten crear sistemas de defensa que se adaptan a crecientes amenazas, reduciendo la intervención humana y mejorando la respuesta ante ataques peligrosos. Esto se relaciona con la IA y la protección de datos digitales al resaltar la necesidad de marcos legales y técnicos que permitan a las defensas digitales anticiparse, adaptarse y contener a crecientes amenazas. La metodología cualitativa de revisión documental y comparativa, en la cual se emplea un diseño que examina y compara modelos y técnicas de IA en áreas clave como detección de amenazas, seguridad de endpoints, phishing, de redes y autenticación adaptativa. El principal hallazgo demostró que los modelos de inteligencia artificial aplicados a la ciberseguridad son eficaces frente a ataques complejos y resaltando la necesidad de mantener defensas sólidas y adaptativas en el entorno digital actual. La IA es vital para fortalecer la seguridad en lo digital y es indispensable actualizar las leyes ante los desafíos tecnológicos presentes.

Rasyid et al. (2024). Explica la "Teoría de la Regulación Jurídica de la inteligencia artificial ante los vacíos normativos en la Seguridad Digital¨, donde argumenta cómo la inteligencia artificial ha reconfigurado las dinámicas delictivas en el entorno cibernético y como plantea un reto normativo y ético, que introduce nuevas formas de criminalidad como los deep fakes y los fraudes automatizados. La metodología normativa de revisión de instrumentos legales nacionales e internacionales, así como doctrinas jurídicas relacionadas con la regulación de la IA, que permitan identificar vacíos regulatorios y contrastar como distintas jurisdicciones abordan la responsabilidad penal frente a delitos tecnológicos. El principal hallazgo, es la carencia de marcos normativos específicos que regulen el uso de la IA en materia penal y de seguridad digital. El artículo es importante porque visibiliza un problema jurídico real que es la insuficiencia de la legislación actual ante la velocidad del desarrollo tecnológico, donde nos ayuda a estar alerta y buscar soluciones tecnológicas frente a los delitos tecnológicos.

Wang (2020) explica la ¨Teoría Jurídica de la adaptación de derecho penal frente a los ciberdelitos impulsados por la inteligencia artificial¨ precisando que la inteligencia artificial es considerado como un fenómeno disruptivo que reconfigurar la estructura del derecho penal y procesal, donde el cual las normas no pueden permanecer estáticas antes las transformaciones tecnológicas, donde propone una reinterpretación del derecho sustantivo nacional y entender con responsabilidad la relación entre seguridad, justicia y derechos fundamentales . La metodología cualitativa de revisión crítica de textos legales, doctrina penal y literatura académica sobre la inteligencia artificial y ciberseguridad, que examinan cómo las normas penales deben adaptarse ante los nuevos ciberdelitos impulsados por la IA. El principal hallazgo evidencia que la actualización del derecho penal es un factor clave para mantener la eficacia de detección de delitos y protección de derechos en un marco tecnológico cambiante para lograr equilibrio entre seguridad y justicia. El artículo es importante porque nos permite centrarnos en los derechos que actúan de manera sólida y que las leyes contra delitos informáticos

deben ir relacionados con la modernización de la tecnología.

Aguilar (2024) presenta la "Teoría de la digitalización de la justicia penal", que completa el uso de la inteligencia artificial para el análisis de pruebas digitales, ya sea como apoyo a jueces y abogados o con cierto grado de autonomía, siempre en concordancia con principios fundamentales como la presunción de inocencia.

La investigación se apoya en un enfoque cualitativo, utilizando el análisis documental y la comparación normativa, considerando directrices internacionales orientadas a la creación de protocolos para el uso ético de la IA en el ámbito judicial. Los resultados evidencian que la inteligencia artificial puede mejorar la eficiencia y la transparencia en los procesos judiciales, aunque su aplicación implica riesgos asociados a la falta de regulación, lo que destaca la necesidad de garantizar la autenticidad y protección de las pruebas digitales. Este estudio es significativo porque compromete una visión actual del impacto de la IA en la justicia penal y formula un marco normativo que fortalece la regulación y la confianza en las tecnologías digitales dentro del sistema judicial.

Maldonado (2024) en la "Teoría de la transición de la administración pública peruana hacia un modelo digital y algorítmico", expresa que esta transición es incitada por tecnologías como la inteligencia artificial, el big data y el blockchain, con el propósito de mejorar la eficiencia estatal. El estudio se basó en un enfoque cualitativo con perspectiva dogmática y analítica, comparando la legislación peruana con los estándares internacionales. Los hallazgos demuestran que, aunque la digitalización contribuye al fortalecimiento de la gestión pública, aún existen vacíos normativos que amenazan la protección de los derechos digitales.

Este trabajo es significativo porque destaca la necesidad de consolidar un marco legal robusto que garantice la transparencia, la equidad y el respeto de los derechos fundamentales en la administración digital.

Gilbert, et al. (2020) en la "Teoría del aprendizaje profundo para la identificación de software malicioso",Sostuvo que, frente a la creciente cantidad de delitos cibernéticos, las redes neuronales profundas y la inteligencia artificial son capaces de robustecer la seguridad digital.

La metodología cualitativa se fundamenta en el modelo HYDRA, que fusiona la valoración dinámica y estática para detectar patrones de conducta en programas ilegales. Los resultados mostraron que esta perspectiva multimodal, además de aumentar la precisión en la categorización del malware, ayuda a crear sistemas más seguros, lo que robustece las estrategias de ciberseguridad ante asaltos y amenazas. Ya que tiene la capacidad de producir beneficios económicos y sociales, pero también podría ser empleada con propósitos dañinos.

Brundage & Clark (2020), Ellos nos muestran "la teoría de la innovación con doble filo", Dado que puede generar ventajas tanto en lo económico como en lo social, aunque también podría ser aprovechada para fines nocivos como ataques cibernéticos, alteración de datos o el desarrollo de armamento autónomo. La metodología cualitativa busco examinar cuestiones de índole digital, física y de protección. Los resultados revelaron que la lA podría exacerbar los peligros ya existentes, abrir la puerta a nuevas modalidades de ofensivas y complicar su detección y gestión; considerando esto, los autores del estudio proponen que las compañías, los estados y los estudiosos se involucren y fomenten una ética íntegra y consciente para asegurar que la lA se use de manera segura, priorizando el bienestar y la protección de la comunidad.

METODOLOGÍA

2.1 Tipo, enfoque y diseño de la investigación: El análisis realizado incumbe a un tipo básico de investigación, dado que su meta principal no

es el uso inmediato de cambios ni la mediación directa en la realidad (Mendoza 2023), sino más bien la formación de entendimiento teórico acerca de cómo la inteligencia artificial está apreciada y asegurada en la legislación de robos informáticos. El estudio adquiere una perspectiva cualitativa, porque examinan documentos normativos, doctrina, jurisprudencia y charlas con expertos jurídicos, prioritariamente a través del entendimiento y la construcción de sentido, mediante mediciones cuantitativas (Godinez 2023). Este estudio logra captar la dificultad, los matices, las percepciones y las relaciones subyacentes en el ámbito legal.

El diseño de la investigación es no práctico, mientras que no hay manipulación de variables ni atribución de grupos, los casos jurídicos serán observados tal como ocurren en el ejercicio, en ese contexto es no experimental (Hernández 2022). Y la investigación además es teoría fundamentada porque: la información emerge del estudio (normas, charlas, casos) de ellos se aplica un modelo explicativo o teoría adecuada al contexto del problema estudiado (Charmaz 2024) El alcance es descriptivo, porque su finalidad es desarrollar las cualidades y modalidades de las dimensiones de estudio, vacíos, fortalezas y limitaciones del enfoque legal existente sin buscar establecer relaciones causales ni hacer predicciones (Villamin 2024).

2.2. Categorías de estudio: En cuanto a la categoría 1 "Inteligencia artificial", observa a fondo cómo la IA está revolucionando la esencia de los delitos cibernéticos, funcionando igual de bien para cometerlos que para pelear contra ellos, sin dejar de lado los dilemas éticos y normativos que se derivan de su uso en los sistemas de ciberseguridad (Achuthan et al., 2024). La IA nos muestra un paradigma dual donde se puede usar para automatizar ataques cibernéticos más complejos a través de métodos de aprendizaje automático, pero a su vez, para crear sistemas de defensa adaptativos y predictivos con habilidades de detección al instante (Kwentoa, 2025). Las subcategorías: Aplicaciones de IA en delitos cibernéticos y peligros; vulnerabilidades relacionadas. Los indicadores: Estrategias como el phishing y los deepfakes; riesgos nuevos y vulnerabilidades provocadas por adversarios. En la categoría 2, denominada "Protección digital", se incluye un amplio rango de estrategias tecnológicas, normativas legales y métodos prácticos orientados a salvaguardar la información digital, los sistemas informáticos y la infraestructura vital frente a las amenazas cibernéticas, asegurando así la confidencialidad, la integridad y la disponibilidad de la información, y al mismo tiempo respetando los derechos fundamentales a la privacidad (AllahRakha, 2024). Este ámbito abarca tanto las medidas tecnológicas destinadas a prevenir incidentes como los modelos regulatorios internacionales que establecen estándares mínimos de seguridad y definen cómo debe actuarse ante un posible incidente (Parambil et al., 2024). Las subcategorías: Técnicas de protección y ciberseguridad; privacidad y protección de datos. Los indicadores: Cumplimiento de normativas en seguridad; nivel de confianza en la seguridad de plataformas digitales.

2.3. La unidad de análisis estuvo conformada por informes estadísticos y artículos científicos especializados en inteligencia artificial, protección digital y legislación sobre delitos informáticos. La población se caracterizó por ser indefinida, debido a la amplitud de fuentes disponibles en bases de datos académicas; por ello, se empleó un muestreo no probabilístico, intencionado y por conveniencia, seleccionando los materiales más pertinentes, recientes y accesibles para los fines del estudio. Criterios de inclusión para el caso del informe estadístico fueron: (i) Relación directa con la dimensión inteligencia artificial, ciberseguridad y legislación sobre delitos informáticos; (ii) Procedencia institucional confiable; y (iii) publicados a partir del año 2020. Los criterios de inclusión para los artículos científicos fueron: (i) publicaciones arbitradas con artículos académicos para garantizar rigor académico; (ii) Relación con aspectos legales, éticos o tecnológicos de la inteligencia artificial

y la protección digital y, (iii) estudios publicados entre el año 2024 y 2025. La muestra se conformó por tres artículos académicos (Jan & Bashir, 2025; Czaja et al., 2025; Arméstar Bruno & Toche Vega, 2024) los cuales permitieron analizar los principales desafíos tecnológicos y vacíos normativos en el ámbito de la ciberseguridad.

2.4. Técnica e instrumentos de recolección de datos: La técnica es el proceso seleccionado para revisar, interpretar y organizar la información recolectada, en este caso el análisis documental (Jan & Bashir, 2025; Czaja et al., 2025; Arméstar Bruno & Toche Vega, 2024). El instrumento empleado la ficha técnica de análisis documental que se caracterizó con contener la siguiente data: Código del documento, fecha y hora de análisis, objetivo de estudio, referencia bibliográfica en APA, tipo de documento, tema principal, categoría y subcategoría de análisis, citas textuales relevantes, resumen del contenido, interpretación crítica del investigador y las observaciones adicionales, (credibilidad, limitaciones, relación con otras fuentes).

2.5. Los aspectos éticos: Los aspectos éticos que se cumplen en este trabajo se ajustan a lo establecido en el Código de Ética. Se advierte la honestidad intelectual científica porque se reconocen las ideas y aportes de otros autores citados (Helgesson & Bülow, 2023). Se cumple la veracidad, justicia y responsabilidad toda vez que se presentan los resultados basados en información real y comprobable (Díaz-Rodríguez et al., 2023). Se respeta la propiedad intelectual porque garantiza el uso ético y legal de la información, respetando los derechos de autor al emplear fuentes académicas, normativas y tecnológicas conforme a las licencias y citaciones establecidas (Díaz, 2025). Empleo de normas APA; ejercicios TURNITIN y reportes IA.

RESULTADOS Y DISCUSIÓN

Para el objetivo general se analizó el artículo "Enfrentando el Robo de Identidad Potenciado por IA: Fortaleciendo los Marcos Legales en India" de Jan & Bashir (2025) el cual examina de qué manera la inteligencia artificial ha hecho que el robo de identidad se convierta en un delito más complicado de manejar, gracias al uso de técnicas como deepfakes, identidades artificiales, phishing automatizado y clonación de voz, herramientas que superan las capacidades de respuesta de legislaciones como la IT Act 2000, la Aadhaar Act 2016 y la Digital Personal Data Protection Act 2023, las cuales no fueron elaboradas para enfrentar las amenazas de los algoritmos actuales. Entre los resultados de la investigación, se destaca un aumento notable en los ataques impulsados por IA que afectan tanto a individuos como a instituciones y organismos gubernamentales, con ejemplos concretos que muestran cómo las autoridades carecen de tecnología avanzada para identificar y seguir los delitos basados en algoritmos, lo que resulta en vacíos significativos tantos operativos como legales.

El artículo argumenta que el robo de identidad relacionado con la IA representa un problema estructural en India y que solo a través de reformas legales específicas, mejora de capacidades tecnológicas, educación digital y cooperación entre el gobierno, la industria privada y la comunidad internacional se podrá establecer un sistema de protección sólido frente a los nuevos peligros que trae la inteligencia artificial.

Para el primer objetivo específico se analizó el artículo "Desafíos y oportunidades de ciberseguridad de las máquinas inteligencia artificial basada en el aprendizaje" de Czaja et al. (2025) el cual da a conocer que la inteligencia artificial como el Machine Learning, está mejorando la ciberseguridad al detectar ataques cibernéticos con mayor precisión. Esto resulta ser muy útil en situaciones de intrusiones, malware, phishing, spam, IoT y en la nube. Sin embargo, hay riesgos asociados, como la manipulación del entrenamiento, ataques adversarios y posibles filtraciones de información. Además, informa que el Machine Learning refuerza la seguridad, pero es necesario implementar nuevas medidas

para proteger la información y prevenir abusos. Este hallazgo se conecta con la Teoría Sistémica y Cognitiva aplicada al internet de las cosas (IoT). Rawlings, L. (2023) señala que la susceptibilidad de los usuarios a correos electrónicos fraudulentos suele incrementarse cuando depositan demasiada confianza en remitentes familiares, se sienten sobrecargados de información o carecen de la formación necesaria para reconocer intentos de estafa. Esto está vinculado a los principios de Protección de Datos Personales, que tienen como objetivo garantizar la información y prevenir su uso inapropiado.

El texto enfatiza que es fundamental implementar medidas técnicas para salvaguardar los datos, tales como controles de acceso, métodos de privacidad, criptografía liviana y sistemas de autenticación más fiables. En términos generales, se enfatiza que la vulnerabilidad al phishing depende tanto del comportamiento y la preparación del usuario, como de las herramientas tecnológicas que lo apoyan. En este contexto, el Machine Learning no solo optimiza la identificación de amenazas y refuerza la seguridad, sino que también crea múltiples riesgos que demandan una protección adicional. Asimismo, enfatiza que la seguridad está determinada tanto por la tecnología como por el comportamiento y la preparación de los usuarios frente a estas amenazas. Por lo tanto, es esencial fortalecer los sistemas y la formación para conseguir una defensa más robusta y eficaz.

Para el segundo objetivo específico, se llevó a cabo una evaluación del trabajo "El tratamiento del fraude informático: un análisis jurídico comparativo entre Perú y Estados Unidos", de Arméstár & Toche (2024). El artículo muestra que, a causa de los progresos en la tecnología digital y las innovadoras metodologías impulsadas por la inteligencia artificial,Estos resultados están vinculados con las ideas de la seguridad digital y la gobernanza tecnológica, las cuales destacan que es necesario revisar los marcos regulatorios frente a nuevas amenazas y reforzar la capacidad institucional para reaccionar; Asimismo, las investigaciones en ciberseguridad apuntan a que la automatización de ataques y el hurto de identidad incrementan la fragilidad de los usuarios y son más efectivos que los métodos tradicionales de protección; esto demuestra que se necesitan medidas preventivas, de supervisión y verificación más sólidas.En términos generales, el artículo señala que la inteligencia artificial ha empeorado el fraude cibernético y que, aunque su impacto en Perú y Estados Unidos es similar, los dos países deberán actualizar sus leyes y mejorar sus capacidades técnicas e institucionales para asegurar una defensa eficaz frente a estos nuevos tipos de delitos digitales.

CONCLUSIONES

Se concluyó, en relación con el objetivo general, que los mayores desafíos para que la inteligencia artificial contribuya al fortalecimiento de la protección digital están vinculados al ritmo acelerado de desarrollo tecnológico, el cual supera la capacidad del derecho penal para actualizarse. A partir del análisis documental y tomando como referencia la "Teoría de la innovación con doble filo" planteada por Brundage & Clark (2020), se evidenció que, si bien la IA genera valor económico y social, su uso indebido en ciberataques o en la creación de deepfakes incrementa los riesgos existentes y complica su regulación jurídica. Se identificó además que la legislación actual sobre delitos informáticos presenta vacíos relevantes respecto a la responsabilidad civil y penal asociada a sistemas automatizados, lo que provoca incertidumbre normativa y debilita la confianza pública en la administración de justicia frente a nuevas modalidades delictivas.

Con respecto al primer objetivo específico, se determinó que las aplicaciones contemporáneas de IA, especialmente aquellas basadas en Machine Learning, exigen la adopción urgente de medidas de protección y ciberseguridad más sólidas y adaptables. El análisis se apoyó en la Teoría Sistémica y Cognitiva presentada por Rawlings (2023), la cual señala que la vulnerabilidad digital no solo depende de aspectos técnicos, sino que

se intensifica cuando los usuarios depositan demasiada confianza en contactos conocidos o carecen de habilidades para reconocer fraudes automatizados. Como resultado, se concluyó que los mecanismos tradicionales ya no bastan, y que se requiere incorporar esquemas avanzados de control de acceso (como RBAC y autenticación multifactor) junto con soluciones de criptografía ligera capaces de resguardar los modelos de IA frente a ataques adversarios y alteraciones de datos.

Respecto al segundo objetivo específico, se verificó que los mecanismos actuales de ciberseguridad y protección digital no son suficientes frente a amenazas emergentes como la clonación de voz o los deepfakes. Los hallazgos mostraron que la sofisticación de estas técnicas permite a los ciberdelincuentes evadir los sistemas tradicionales de seguridad, dificultando tanto la identificación de los responsables como la verificación de autenticidad. En consecuencia, se evidenció la urgencia de actualizar el marco legal y reforzar las capacidades institucionales y técnicas, alineándose con estándares internacionales y promoviendo una gobernanza tecnológica que permita anticipar y gestionar estas amenazas. Con ello se busca salvaguardar de manera efectiva los derechos fundamentales en el entorno digital.

REFERENCIAS BIBLIOGRÁFICAS

Achuthan, K., Jha, S., Prabaharan, S., Nair, S., Francis, S., Shabbiha, S., & Mishra, D. (2024). Advancing cybersecurity and privacy with artificial intelligence: Literature review and analysis. PLoS ONE, 19(12), e0313766. https://doi.org/10.1371/journal.pone.0313766

Aguilar, D. (2024). La inteligencia artificial en la justicia: Protocolos para la presentación y la valoración de prueba digital obtenida mediante IA. Revista Oficial del Poder Judicial, 16(22), 475–497. https://doi.org/10.35292/ropj.v16i22.1018

Aleke, N. (2024). The Role of Cybersecurity Legislation in Promoting Data Privacy. En Advances in information security, privacy, and ethics book series (pp. 205-244). https://doi.org/10.4018/979-8-3373-0588-2.ch008

AllahRakha, N. (2024). Cybersecurity Regulations for Protection and Safeguarding Digital Assets (Data) in Today's Worlds. Lex Scientia Law Review, 8(1). https://doi.org/10.15294/lslr.v8i1.2081

Alkaabi, A., Mohay, G., McCullagh, A., & Chantler, N. (2011). Dealing with the Problem of Cybercrime. En Springer eBooks (pp. 1-18). https://doi.org/10.1007/978-3-642-19513-6_1

Alsamara, T., & Ghazi, F. (2024). The Steady Development of Digital Law: New Challenges of Artificial Intelligence. Journal Of Ecohumanism, 3(5), 1096-1102. https://doi.org/10.62754/joe.v3i5.3957

Arias, F. (2020). El proyecto de investigación científica. Episteme.

Arméstar Bruno, G., & Toche Vega, F. (2024). El tratamiento del fraude informático: un estudio del derecho comparado entre Perú y Estados Unidos. La Voz Jurídica. https://doi.org/10.53870/lvj.390

Boato, G., Pasquini, C., Stefani, A., Verde, S., & Miorandi, D. (2022b). TrueFace: a Dataset for the Detection of Synthetic Face Images from Social Networks. Institute Of Electrical And Electronics Engineers Inc. https://doi.org/10.1109/ijcb54206.2022.10007988

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., … & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228. https://doi.org/10.48550/arXiv.1802.07228

Chatinakrob, T. (2024). Legal Risks and Challenges of Unregulated AI. En Brill |

Nijhoff eBooks (pp. 268-315). https://doi.org/10.1163/9789004719934_010

Concha Flores, L. (2024). Inteligencia artificial, enfoque de riesgos y responsabilidad civil: aspectos centrales para una razonabilidad práctica. SAPIENTIA IURIS, Nº 1, 140-169. https://doi.org/10.5281/zenodo.14735552

Chen, Y., Gao, X., & Wu, X. (2021). Application of AI Technology in Defense of Big Data Network Security. Journal Of Physics Conference Series, 1802(3), 032105. https://doi.org/10.1088/1742-6596/1802/3/032105

Charmaz, K. (2024). Constructing grounded theory (3rd ed.). SAGE Publications. https://uk.sagepub.com/en-gb/eur/constructing-grounded-theory/book255601

Czaja, P., Gdowski, B., Niemiec, M., Mees, W., Stoianov, N., Votis, K., Kharchenko, V., Katos, V., & Merialdo, M. (2025). Desafíos y oportunidades de ciberseguridad de las máquinas inteligencia artificial basada en el aprendizaje. Computación Neuronal y Aplicaciones, 37, 27931–27956. https://doi.org/10.1007/s00521-025-11604-9

Das, S., Balmiki, A., & Mazumdar, K. (2022). The Role of AI-ML Techniques in Cyber Security. En Advances in information security, privacy, and ethics book series (pp. 35-51). https://doi.org/10.4018/978-1-6684-3991-3.ch003

Defensoría del Pueblo (2024). Reporte Regional: Uso de inteligencia artificial y salvaguarda digital en las leyes sobre delitos cibernéticos. Fundado en el Informe Defensorial Nº 001-2023. https://www.inei.gob.pe/media/MenuRecursivo/boletines/boletin_seguridad_ciudadana_dic24-may25.pdf

Díaz, "Digital privacy and the law: the challenge of regulatory capture". AI & Society, 40, 2777-2787 (2025). https://doi.org/10.1007/s00146-024-02041-8

Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., López de Prado, M., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the Dots in Trustworthy Artificial Intelligence: From AI Principles, Ethics, and Key Requirements to Responsible AI Systems and Regulation. (preprint) arXiv. https://doi.org/10.48550/arXiv.2305.02231

Gibert, Mateu; Planes (2020) HYDRA: A multimodal deep learning framework for malware classifictiona.https://doi.org/10.1016/j.cose.2020.101873

Helgesson, G., & Bülow, W. (2023). Research Integrity and Hidden Value Conflicts. Journal of Academic Ethics, 21, 113-123. https://doi.org/10.1007/s10805-021-09442-0

Hernández-Sampieri, R., & Mendoza, C. (2022). Metodología de la investigación: Las rutas cuantitativa, cualitativa y mixta (7ª ed.). McGraw-Hill Education. https://virtual.cuautitlan.unam.mx/rudics/?p=2612

Jan, S & Bashir, A. (2025) Combating AI-Enabled Identity Theft: Strengthening Legal Frameworks in India. Journal Of Intellectual Property Rights, 30. https://doi.org/10.56042/jipr.v30i5.15633

Kavitha, D., & Thejas, S. (2024b). AI Enabled Threat Detection: Leveraging Artificial Intelligence for Advanced Security and Cyber Threat Mitigation. IEEE Access, 1. https://doi.org/10.1109/access.2024.3493957

King, T., Aggarwal, N., Taddeo, M., & Floridi, L. (2020). Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions. Science and Engineering Ethics, 26, 89–120.120 https://doi.org/10.1007/s11948-018-00081-0

Kshirsagar, V., Pachpor, N., Suryawanshi, S., Chavan, T., Nair, N., Agrawal, P., & Shahane, T. (2025). Artificial Intelligence powered Crime Scene Analysis Service. MethodsX, 15, 103430. https://doi.org/10.1016/j.mex.2025.103430

Kwentoa, I. (2025). AI-Driven Threat Intelligence for Enterprise Cybersecurity. Journal Of Next-Generation Research 5.0. https://doi.org/10.70792/jngr5.0.v1i4.125

Lee, G., Latif, E., Wu, X., Liu, N., & Zhai, X. (2024). Applying large language models and chain-of-thought for automatic scoring. Computers And Education Artificial Intelligence, 6, 100213. https://doi.org/10.1016/j.caeai.2024.100213

Ling Wu, Qiong Peng y Michael Lembke (2023). Research trends in cybercrime and cybersecurity: A review based on Web of Science core collection database. International Journal of Cybersecurity Intelligence and Cybercrime, 6(1), 5-28. https://doi.org/10.52306/OZMB2721

Martín Ramos, C. (2024). Cybersecurity and artificial intelligence (AI). South Florida Journal of Development, 5(8), e4276. https://doi.org/10.46932/sfjdv5n8-021

Maldonado-Meléndez, M. (2024). El tránsito de la administración digital hacia una administración pública algorítmica en la era de la inteligencia artificial: La necesidad de un ordenamiento jurídico constitucional y legal garantista en la prestación de servicios públicos en el Perú. Revista de Derecho Político, (120), 395–425. https://doi.org/10.5944/rdp.120.2024.41775

Mejía Arbildo, T. (2023). Inteligencia artificial y sus efectos en la protección de datos personales en la Ley N.º 29733 https://alicia.concytec.gob.pe/vufind/Record/UCVV_1753c320c381e6636c11b1a0e2648184/Details

Murrugarra, B. (2025). Inteligencia artificial y privacidad en internet: Amenazas para los datos personales de los usuarios. Universidad César Vallejo. https://doi.org/10.69516/9dp8ap45

Nurmansyah, G., Wiranata, I., Fardiansyah, A. & Mladenov, S. (2024). Preventing AI-based phishing crimes across national borders through the reconstruction of personal data protection laws. Jurnal Hukum Novelty, 15(2), 286-311. https://doi.org/10.26555/jhn.v15i2.27558

Novelli, C., & colaboradores. (2024). A robust governance for the AI Act: AI Office, AI Board, Scientific Panel, and National Authorities. European Journal of Risk Regulation. https://www.cambridge.org/core/journals/european-journal-of-risk-regulation/article/robust-governance-for-the-ai-act-ai-office-ai-board-scientific-panel-and-national-authorities/98FEE97C8F9423DFCC28CBE063F9753B

Paisal, M. (2025). El uso de la inteligencia artificial en la investigación policial y judicial de delitos de online child sex grooming en España. IDP Revista de Internet Derecho y Política, 0(42), 1-12. https://doi.org/10.7238/idp.v0i42.430914

Parambil, M., Mathew, S., & Cavus, N. (2024). Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and prospects. Computers and Education: Artificial Intelligence, 6, 100213. https://doi.org/10.1016/j.caeai.2024.100213

Quinn, K., Stukel, T., Detsky, A., Chung, H., Anwar, M., Bhatia, S., Downar, J., Hung, V., Isenberg, S., Kurahashi, A., Lee, D., Stall, N., Tanuseputro, P., & Bell, C. (2025). Use of virtual care near the end of life before and during the COVID-19 pandemic: A population-based cohort study. PLoS ONE, 20(1), e0313766. https://doi.org/10.1371/journal.pone.0313766

Rasyid, M., Akhdharisa, M., SJ, Mamu, K., Paminto, S. R., Hidaya, W. A., & Hamadi, A. (2024c). Cybercrime Threats and Responsibilities: The Utilization of Artificial Intelligence in Online Crime. Jurnal Ilmiah Mizani Wacana Hukum Ekonomi Dan Keagamaan, 11(1), 49. https://doi.org/10.29300/mzn.v11i1.3318

RPP Noticias. (2025, 9 de marzo). Ciberdelincuencia en Perú aumentó un 40%

en 2024. RPP. https://rpp.pe/peru/actualidad/fraudes-digitales-y-suplantacion-de-identidad-alarmantes-cifras-de-la-pnp-revelan-el-impacto-de-la-ciberdelincuencia-en-peru-noticia-1620466

Siam, A., Alazab, M., Awajan, A., & Faruqui, N. (2025). A Comprehensive Review of AI's Current Impact and Future Prospects in Cybersecurity. IEEE Access, 1. https://doi.org/10.1109/access.2025.3528114

Tropina, T. (2020). Cybercrime. En Routledge eBooks (pp. 148-160). https://doi.org/10.4324/9781351038904-14

Taddeo, M., & Floridi, L. (2021). How AI can be a force for good. Science, 361(6404), 751–752. https://doi.org/10.1126/science.aat5991

Veale, M., & Borgesius, F. (2021). Demystifying the draft EU Artificial Intelligence Act. Computer Law Review International, 22(4), 97–112. https://doi.org/10.9785/cri-2021-220402

Villamin, P., López, V., Thapa, D., & Cleary, M. (2024). A worked example of qualitative descriptive design: A step-by-step guide for novice and early career researchers. Journal of Advanced Nursing. https://doi.org/10.1111/jan.16481

Wang, X. (2020). Criminal Law Protection of Cybersecurity Considering AI-based Cybercrime. Journal Of Physics Conference Series, 1533(3), 032014. https://doi.org/10.1088/1742-6596/1533/3/032014

Wiafe, I., Koranteng, F., Obeng, E., Assyne, N., Wiafe, A., & Gulliver, S. (2020). Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. IEEE Access, 8, 146598-146612. https://doi.org/10.1109/access.2020.3013145

Zabala Leal, T., & Gómez Macfarland, C. (2024). La responsabilidad civil y la ética en la inteligencia artificial: una revisión sistemática de las ideas del período 2018-2023. IUSTA, 60, 66-93. https://doi.org/10.15332/25005286.9964

Zahra, A., & Nurmandi, A. (2021). The Strategy of Develop Artificial Intelligence in Singapore, United States, and United Kingdom. IOP Conference Series Earth And Environmental Science, 717(1), 012012. https://doi.org/10.1088/1755-1315/717/1/012012