ARTÍCULO DE REFLEXIÓN

Cibercrimen: Un breve análisis doctrinal de los ciberdelitos y su relación con la inteligencia artificial

Cybercrime: A brief doctrinal analysis of cybercrimes and their relationship with artificial intelligence

Leónidas Salvador Tapia Sánchez[1]
Keiser University Latin American Campus

Recibido: 25.01.2025
Aceptado: 15.03.2025

Resumen

La humanidad por medio de la tecnología ha llegado a límites que, siglos atrás, eran considerados utópicos o irreales. La presente investigación se basa en el análisis del diseño y desarrollo emergente de la Inteligencia Artificial o IA, concepto acuñado desde el año 1956 por John McCarthy, pero que ha ido ganando campo dentro de la sociedad actual, con herramientas para uso académico, laboral o social, como el famoso ChatGPT. Por lo tanto, se aborda también la forma en que mediante herramientas de IA se crean fake news o noticias falsas que desinforman a la población con el objetivo de crear caos o distorsionar la realidad; así como deepfakes que imitan la voz, imagen o ciertos patrones de una persona o grupos de personas para cometer estafas en internet, como las romances cam, phishing, doxxing, suplantación y robo de identidad. Asimismo, se abordan y analizan otros aspectos relacionados con la cibercriminalidad y la ciberseguridad. El corolario de esta investigación,

[1] leonidas.tapia@keiseruniversity.edu
https://orcid.org/0000-0002-9711-720X

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

con relación a los objetivos planteados, fue que, efectivamente la Inteligencia Artificial o IA tiene especial participación en la comisión de ciertos ciberdelitos, que la misma es un coadyuvante no un autor de ciberdelitos, y que, a contrario sensu, también existen herramientas de IA que son utilizadas para la persecución e investigación del cibercrimen.

Palabras clave: inteligencia artificial, ciberdelitos, redes sociales, ciberseguridad, TIC

Abstract

Humanity through technology has reached limits that, centuries ago, were utopian or unrealistic. This research is based on the analysis of the design and emerging development of Artificial Intelligence or AI, a concept coined since 1956 by John McCarthy, but which has been gaining ground within today's society, with tools for academic, work or social use, such as the famous ChatGPT. Therefore, it also addresses the way in which AI tools create fake news that misinforms the population with the aim of creating chaos or distorting reality; as well as deepfakes that imitate the voice, image or certain patterns of a person or groups of people to commit scams on the internet, such as romance scam, phishing, doxxing, and identity theft or impersonation. Likewise, the aspects are addressed and analyzed, as well as others related to cybercrime and cybersecurity. The corollary of this research, in relation to the objectives set, was that, indeed, Artificial Intelligence or AI has a special participation in the commission of certain cybercrimes, that it is an adjuvant not a perpetrator of cybercrimes, and that, a contrario sensu, there are also AI tools that are used for the investigation of cybercrime.

Keywords: artificial intelligence, cybercrime, social media, cybersecurity, ICT

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

Introducción

El presente trabajo investigativo es de carácter teórico, con enfoque cualitativo, y en el mismo se plantean los siguientes objetivos: Analizar aspectos conceptuales sobre ciberespacio y ciberdelitos; Explicar cómo la Inteligencia Artificial o IA se relaciona con la comisión de ciberdelitos; Identificar la forma en que la misma Inteligencia Artificial o IA a través de herramientas ad hoc, puede coadyuvar en la investigación del cibercrimen. Por ende, el objeto de estudio es la Inteligencia Artificial o IA y su relación con el cibercrimen. Todo lo antes planteado, a partir de la siguiente pregunta de investigación: ¿Cómo se realizan ciberdelitos con herramientas de Inteligencia Artificial o IA?

De conformidad al carácter teórico de este trabajo, se utiliza la técnica de la investigación documental. Los métodos de investigación aplicados son el lógico-deductivo, el teórico y el hermeneútico, todos con un enfoque cualitativo, para que el lector aprenda sobre la conceptualización de los ciberdelitos, tipos de ciberdelitos y modus operandi de los que participan en la comisión de estos, sin perjuicio de la intervención de la mencionada Inteligencia Artificial o IA en tales actos.

La presente investigación logró determinar la importancia práctica que tiene y que podrá tener a futuro el uso de herramientas de Inteligencia Artificial o IA en la comisión de ciberdelitos, lo cual, incluso podría cambiar los paradigmas jurídicos y doctrinarios establecidos para la aplicación, persecución y castigo de estos.

La Inteligencia Artificial o IA influye en la comisión de ciberdelitos que afectan el patrimonio y el honor; sin embargo, pueden existir otros estudios que indiquen y demuestren que aquella puede dañar diferentes bienes jurídicos tutelados o derechos humanos además de los acá mencionados, por lo tanto, queda mucho por investigar en este tema, especialmente por el avance disruptivo que la IA está teniendo y que, a corto o mediano plazo, puede influir más en la creación, fortalecimiento y comisión de nuevas ciber amenazas y ciberdelitos.

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

1. El ciberespacio: aspectos generales

Las Redes Sociales, los GPS, smartphones, tablets, ordenadores, hasta los wireless earbuds son algunos de los instrumentos tecnológicos básicos en el día a día de las personas, en países desarrollados y en vías de desarrollo. Por tal razón, en el primer capítulo de esta investigación se abarcarán las bases de este nuevo modus vivendi, que nace y se desarrolla en y desde el denominado ciberespacio.

1.1 Ciberespacio y virtualidad

El término ciberespacio tiene relación con la palabra virtualidad porque se entiende como algo irreal, que solamente existe en el pensamiento. Es símil al término "noúmeno" introducido por Kant, es decir, la idea que es inmaterial y descorporizada.

Respecto a ello, "Aunque los noúmenos no están en el espacio-tiempo, su existencia es un hecho, un hecho suprasensible. La realidad ontológica noumenal que trasciende lo espacio-temporal se nos presenta en primer lugar e inmediatamente en la propia libertad." (Rosas, 2016, 30).

Lo que se lleva a cabo dentro del ciberespacio tiene una consecuencia para quienes navegan en él, e igualmente para quienes se encuentran fuera. Lo que se expresa desde aquel, trasciende en el resto de los cibernautas, en el mundo real.

He ahí la lógica que desde el ciberespacio se pueden cometer actos que afectan el mundo material como una amenaza terrorista, un hackeo masivo de ordenadores, o una estafa, dirigida o en masa; y esto sucede sin contacto físico en lo que respecta al sentido del tacto o el olfato, no así en lo atinente a los otros sentidos, como la vista y el oído.

Según el Informe Digital de la web We Are Social (2024), a enero del 2024, la población global era de 8,08 billones. De estas, 50,2 por ciento hombres y 49,8 por ciento mujeres. En

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

general, el gasto en tiempo per cápita y por día rondaba las 6 horas con 40 minutos en internet; y respecto al uso de las redes sociales, el tiempo rondaba las 2 horas y 23 minutos. Y las principales razones por las cuales las personas se conectan a internet están, la búsqueda de información (60.9%) y estar en contacto con amigos (56.6%).

Por su parte, Galán Muñoz (2019), refiere que el imparable desarrollo de sistemas informáticos ha logrado calar en todas las facetas de la humanidad, porque se trabaja con ordenadores, la comunicación es por correo electrónico o mensajería de datos, y se controla la banca por algoritmos y aplicaciones que se llevan en los teléfonos móviles. Igualmente, se realiza oferta y demanda a través de dispositivos electrónicos y se tiene acceso a todo tiempo de contenido por medio de las redes sociales.

Dentro de este nuevo paradigma de desarrollo humano, surge también un nuevo concepto de activo, el cual es digital, y es un bien jurídico protegido. Verbigracia: el dato personal, una cuenta bancaria o patrimonio digital, entre otros. Todo fortalecido por el comercio electrónico y el almacenamiento de inmensas bases de datos, siendo parte elemental de ello, los datos personales.

Esto ha ocasionado, directa o concomitantemente, que los delitos virtuales o ciberdelitos tengan mayor convergencia y peligrosidad por las vulnerabilidades en el uso y manejo de datos por parte de los usuarios en internet.

Verbigracia, en ciertas transacciones en línea, el cliente y el comercio no hablan de forma sincrónica, sino que ciñen su relación a una aplicación o plataforma digital que, aplicando machine learning, el chatbot, obtiene más información para dar una respuesta acorde a las necesidades de los clientes y llegar a un acuerdo. La información del cliente se almacena y, en muchos casos se comparte.

Todo ello crea grandes bases de datos o Big Data, lo cual constituye para los cibercriminales un inconmensurable ecosistema donde pueden afectar a sus moradores digitales; verbigracia,

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

a través de phishing, carding, ransomware o doxxing, etcétera, los cuales también pueden auxiliarse de la IA en su caso.

1.2 Ciberdelitos: aspectos conceptuales y características

Los ciberdelitos son actos típicos y antijurídicos realizados en o desde el ciberespacio. Son cometidos por ciberdelincuentes, quienes aprovechan las transacciones o envíos de dinero, la exposición o manejo imprudente de información en redes sociales, la información publicada en plataformas en línea, etcétera.

Ruiz & Cortés Borrero (2023) reputan a los ciberdelitos como actividades ilícitas llevadas a cabo por medio de internet. Nacieron desde la década de los cuarenta del siglo pasado, en donde se desarrollaron las primeras redes informáticas, que también requerían de sistemas de seguridad, hoy denominado, ciberseguridad.

En este contexto, la IBM, hacia el año 1967, recurrió en su momento a estudiantes o hackers para determinar vulnerabilidades en la nueva computadora que había creado, dando origen a lo que se conoce hoy en día como Hacking Ético.

Ruiz & Cortés Borrero (2023), aducen que en la década de los noventa y el desarrollo global del Internet, se originan una serie de nuevos ciberdelitos como el robo de identidad, el phishing y el ransomware.

Debido a ello, el derecho penal otorga a los ciberdelitos la equivalencia respecto a los delitos comunes, máxime en aquellas nuevas modalidades delictivas que se van creando o fortaleciendo con la ayuda de la IA o Inteligencia Artificial.
Según Gercke (2014), la introducción de las TIC ha acuñado el concepto de sociedad de la información, y los adelantos técnicos han mejorado la vida diaria, no obstante, dicho crecimiento está acompañado de graves amenazas emergentes.

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

Entre tales amenazas, surgen también aquellas que atacan infraestructura informática, como virus o los denominados malwares. A ello se le suma el desarrollo de la precitada Inteligencia Artificial o IA, utilizada con fines inicuos.

Desde la segunda mitad del siglo XX y los primeros 25 años del siglo XXI, con el mencionado desarrollo tecnológico, Cumpa González (2012), deduce en lo siguiente:

> La llegada de las tecnologías digitales viene transformando diversos campos de la comunicación, entre ellos las formas de elaboración de los contenidos verbales, visuales y multimediales. Esto ha generado una forma de comunicación distinta en algunos espacios de transmisión de la información que las tecnologías digitales ponen a disposición de millones de usuarios, como lo son, principalmente, las redes sociales caracterizadas por su manera de acceder a ellas (la movilidad de esos medios) (p. 128).

Asimismo, según Cumpa González (2012), los signos lingüísticos, gestos, formas, colores, entre otros, articulados de formas diferentes generan muchas variaciones que al mismo tiempo conciben posibilidades muy amplias para la forma en que las personas se comunican en estos tiempos lo que facilita la comisión de ciberdelitos, cuyas características serán analizadas a continuación.

Descorporización

En los ciberdelitos, el autor no está presente físicamente, o frente a la víctima. Se diferencian de los delitos que requieren contacto físico, o, mejor dicho, delitos comunes como el robo y sus diferentes modalidades, la violación, las lesiones físicas, el homicidio y sus agravantes, entre muchos otros.

La página web Gestión (2016), de conformidad a datos recopilados por Digiware que es un integrador de seguridad informática en América Latina, las grandes organizaciones criminales alrededor de todo el mundo atacan aproximadamente 600.000 veces por día, sobre todo, al

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

sector financiero y de gobierno, y tales ataques se realizan a distancia, incluso desde otros países.

Atemporalidad y deslocalización

Igualmente, en la comisión de ciberdelitos puede que la acción tenga una hora o momento determinado y el resultado se dé en otro momento o lugar, lo cual puede generar competencia en ambos espacios o lugares. Por ejemplo, enviar una cantidad considerable de virus informáticos a diferentes empresas localizadas en diferentes países o jurisdicciones, mediante email, ocasionaría un daño considerable dependiendo del resultado, el cual se daría en tiempos y lugares diferentes, siendo lo último, el aspecto relacionado con la deslocalización.

En el ciberespacio, por consiguiente, los tiempos de acción y resultado varían en muchos casos, así como el lugar de la comisión o del resultado propiamente dicho. En términos jurídicos, la acción se considera realizada cuando el autor logra proceder a través de los actos ejecutivos correspondientes, con la voluntad y tentativa de cometer un ciberdelito.

Verbigracia, un estafador través de internet, vende un servicio que al final es falso, es decir, un scam o estafa en línea, y la víctima ya había pagado mediante una transacción en línea. La acción de estafar se dio mediante el ciberespacio y la lesión al patrimonio igualmente, aunque esta última se materialice en el mundo real, y tanto la víctima como el autor podían encontrarse en lugares diferentes con husos horarios disímiles, lo cual al final constituyen características propias de los ciberdelitos.

Ingeniería Social

Los ciberdelitos basan su actividad también en aspectos de ingeniería social o actos de manipulación de los cibercriminales. De conformidad con el sitio web Gestión (2016), los ciberdelincuentes son personas con conocimientos que otros no tienen sobre todo en materia computacional y de redes, es decir, tienen conocimiento por encima del promedio; son

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

personas que aprovechan los espacios sociales para conocer sobre información secreta o restringida; son capaces de instalar virus o desinstalar antivirus en equipos computacionales, y estos pueden ser trabajadores o extrabajadores de empresas del sector público o privado. Y también son personas con grandes capacidades de persuasión.

Por lo tanto, los ciberdelitos que son cometidos en su mayoría por cibercriminales o ingenieros sociales, utilizan o ponen en práctica lo siguiente: confianza que los usuarios ponen en la seguridad que las plataformas digitales ofrecen, deslocalización, atemporalidad y descorporización, persuasión o capacidad de convencimiento por parte de los ingenieros sociales, capacidad de identificación de vulnerabilidades de las víctimas; y el adecuado manejo de datos e información que circula en redes sociales subida a estas por los mismos usuarios, sin el debido cuidado o la prudencia que el caso amerita.

En conclusión, la ingeniería social, es un método de engaño o manipulación utilizado por ciertas personas que, desde o en el ciberespacio, incluso se presenta con mayor peligrosidad por el anonimato o acicalamiento de los cibercriminales.

2. Inteligencia Artificial (IA) y ciberdelitos

Analizados a priori, los aspectos dogmáticos de ciberespacio, ciberdelitos, y sus características, se procede en el presente apartado a realizar una relación factual de estos con la Inteligencia Artificial o IA, la cual está causando una revolución tecnológica y, a su vez, es un disruptivo dentro de la mencionada sociedad de la información porque es capaz de dar respuestas de forma muy comprensible a las preguntas que se le formulan, en la solución de problemas o interrogantes.

Actualmente, las herramientas de IA están facilitando la investigación, procesamiento y búsqueda de la información, así como la creación de contenidos digitales o computacionales que, en algunos casos, lamentablemente pueden ser herramientas utilizadas para lesionar bienes jurídicos. Por ello, se analiza la Inteligencia Artificial y su relación con los ciberdelitos.

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

2.1 Las TIC y la IA: relevancia en la comisión de ciberdelitos

Miranda Goçalves (2024) explica que esto se genera desde el año 1950, con el "Test de Turing", en el cual, Adam Turing propuso determinar si una máquina podía exhibir un comportamiento inteligente que fuese distinguible del humano. A posteriori, John McCarthy acuñó el término Inteligencia Artificial en 1956.

Los ciberdelitos, por su parte, suponen graves daños a infraestructuras informáticas, patrimonio, la intimidad y privacidad, la economía pública o privada, entre otros bienes jurídicos. Al respecto, Romero Casabona & Rueda Marín (2023), expresan lo siguiente:

> La realidad demuestra que en torno a las TIC y el ciberespacio se ciernen riesgos y amenazas cuya repercusión en la sociedad puede tener elevados costes, entre otras razones por su acusada transversalidad, por lo que recientemente se ha contemplado la intervención del Derecho penal para castigar determinados ataques que suponen una incidencia grave sobre la ciberseguridad (p. 24).

Las TIC suponen el ecosistema de donde se alimentan, crecen y nacen las ideas y actos propios del cibercrimen, en donde la IA también tiene su rol, sin embargo, resulta importante mencionar que la Inteligencia Artificial o IA, también ayuda en la lucha contra el precitado cibercrimen.

En este caso, Zambrano Rendón (2024), citando a Rodríguez (2023), expresa lo siguiente:

> La inteligencia artificial (IA) ha revolucionado de manera significativa numerosos campos en la sociedad moderna, desde la atención médica y la conducción autónoma hasta la optimización de procesos industriales. Sin embargo, este mismo avance tecnológico, que ha traído consigo una amplia gama de beneficios, también ha sido aprovechado por actores malintencionados para perpetrar ciberataques cada vez más sofisticados y peligrosos (p.2).

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

La IA supone una disrupción más avanzada de la tecnología, llegando al punto de suponer que la misma puede desplazar al ser humano a corto o largo plazo. Por ende, los actos que también con la ayuda de la IA se puede realizar, pueden subsumirse en ciberdelitos o delitos conexos, como lo son la suplantación de identidad, el plagio de una obra o de datos personales, entre otros.

En tal sentido, Miranda Gonçalves (2024), expresa lo siguiente:

> La IA no solo ha transformado la vida social, sino que también se viene proyectando de igual manera en los contextos sociales, económicos y políticos. Autores como Becerril advierten que la propia esencia y objetivo que alinea la implantación de agentes de la IA debe tratarse con cautela porque los sistemas basados en IA cuentan con ventajas como la de analizar grandes cantidades de datos y tomar decisiones de forma automatizada, facilitando también nuevas formas de vigilancia y control y con ella, nuevas fenomenologías delictivas (p. 794).

Asimismo, Zambrano Rendón (2024), expresa que el famoso ChatGPT es una de las herramientas de IA que más ha tenido evolución en los últimos años y es tan así, que la misma autora, citando a Galindo (2020), de conformidad con un estudio realizado por la Universidad de Oxford y la Universidad de Yale, se presume que la Inteligencia Artificial superará a los seres humanos en diversas actividades en los próximos diez años.

Por ello, la IA puede ser utilizada para la comisión de ciberdelitos o actos ilícitos en y desde el ciberespacio. A continuación, dicho análisis.

Fake News e IA

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

Las fake news o noticias falsas, hoy en día son comunes, especialmente en redes sociales. Son incluso asimiladas por muchos internautas como algo normal o gracioso. Sin embargo, informarse inadecuadamente o consumir información que no es real puede tener consecuencias graves como lo es la especulación en términos económicos, lo que al mismo tiempo podría causar caos por la presunta escasez de un determinado producto, a cómo ocurrió en varios países al inicio de la pandemia del Covid19, en donde se vieron grandes cadenas de supermercados abarrotadas de personas que se informaron por medio de internet u otros medios de información, de una presunta escasez de productos de primera necesidad.

Zambrano Rendón (2024), citando a Llano (2022), expresa que un grupo de expertos de alto nivel sobre noticias falsas y desinformación de la Unión Europea presentó un Informe sobre las fake news en línea, en el cual se dejó claro la intención maliciosa de estas, dirigida a causar daño público o lograr ventajas particulares.

Por su parte, Todesca (2023), de conformidad a un estudio de la firma Statista, entre abril y mayo del año 2022, el 89% de la población de la Unión Europea afirmó estar expuesta a noticias falsas o desinformación; y de este porcentaje total, un 30% afirmó que tal situación les ocurrió de manera frecuente o muy frecuente.

Asimismo, Todesca (2023) expresa que el uso de la IA para generar fake news se ha ido perfeccionando, por ejemplo, con el mencionado ChatGPT que es el acrónimo de: Generative Pre-trained Transformer. El problema es que, este tipo de IA se alimenta o entrena a través de la información que ella recibe y luego comparte, y en algunos casos, según muchas investigaciones realizadas, existe imprecisión en las respuestas brindadas, lo que puede ser generadora de información o noticias falsas.

Por consiguiente, siguiendo la tesis de Zambrano Rendón (2024), para la creación de fake news, es necesario establecer una fábrica de noticias falsas a través de la creación de un sitio web en donde se alojarán y presentarán dichas noticias, para lo cual se necesita primeramente adquirir un nombre de dominio y luego el servicio de hosting para el sitio web.

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

A posteriori, las redes sociales hacen lo suyo al amplificar y masificar la noticia a través de sus portales que, a como es sabido, son vistos por miles de millones de personas o usuarios activos alrededor del mundo.

Y el estar conectado tanto tiempo por día a internet, especialmente a las redes sociales, configura un riesgo de ser víctima de algún ciberdelito por medio de tácticas de ingeniería social, o de las mencionadas fake news.

En general, según Zambrano Rendón (2024), existen herramientas de IA que se utilizan o pueden ser utilizadas para la generación de noticias falsas, desde contenido per se, hasta imágenes relacionadas con dicho contenido, como lo son el ya mencionado ChatGPT y el Infertik, los cuales generan textos a partir de una descripción que puede venir de una fake news. Asimismo, existen herramientas de IA como Leonardo IA, DALL E, entre otras, las cuales crean imágenes realistas a partir de textos, o los mejor conocidos como deepfakes, los que se analizarán a continuación.

Deepfakes e IA

En lo que respecta a los orígenes de las deepfakes, Zambrano Rendón (2024), expresa, citando a Visus (2021), que sus orígenes datan del año 2014 cuando Ian Goodfellow, un doctorando de la Universidad de Montreal realizó un avance pionero en la generación de imágenes utilizando un proceso denominado GAN por sus siglas en inglés, o redes neuronales generativas adversarias. Su enfoque se basaba en entrenar dos redes neuronales utilizando el mismo conjunto de datos de imágenes y luego emplearlas para generar nuevas imágenes.

En la misma línea, de conformidad a la página web de La Universidad en Internet UNIR (2024), deepfake es un archivo de vídeo, imagen o voz manipulados mediante inteligencia artificial. Se le conoce también como medios sintéticos y es generada con técnicas de machine learning llamadas deep learning, mediante el uso de algoritmos de redes neuronales.

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

Por su parte, también con IA se puede crear e imitar la voz de ciertas personas. En tal sentido, se trae a colación el caso que, según Sadoian (2025), ocurrió en el año 2019 a un ejecutivo de una empresa energética del Reino Unido, en donde el director de esta fue defraudado con 220,000 euros al recibir órdenes por teléfono de su supuesto jefe, las que fueron generadas por IA, y con ello transfirió el dinero a cuentas que le orientaron los estafadores.

Por su parte, Zambrano Rendón (2024), respecto a los deepfakes infiere lo siguiente:

> Kaspersky (2023) los define como videos falsos creados utilizando software digital, aprendizaje automático y la técnica de intercambio de caras. En estos videos, se combinan imágenes para generar nuevas secuencias que representan eventos o acciones que nunca ocurrieron en realidad. Los resultados suelen ser extremadamente convincentes y difíciles de detectar como falsos. La revista Consumer (2023) indica que la desinformación ha alcanzado un nivel más sofisticado con la ayuda de la inteligencia artificial (p. 9).

Con las herramientas de IA, se pueden crear imágenes, textos, paisajes, voces, situaciones o vídeos que son falsos, o que, en la realidad, no sucedieron. Verbigracia, que una persona aparezca dando unas declaraciones en una página de red social en contra de una minoría por razones raciales; o que sea colocada en una presunta filmación de un robo a un banco, todo con IA generativa de deepfakes. Lo más grave supondría que dicha imagen o vídeo, podría inculpar sesgadamente a quien aparece en la misma o, a un tercero, dañando la dignidad u honor de los involucrados. Es un acto que, por consiguiente, deshumaniza.

Aunque la máquina o la herramienta de IA haya generado la noticia, imagen o vídeo falsos, el factor humano estaría detrás, de lo contrario se entraría a un debate jurídico de inmensas proporciones buscando la lógica jurídico-legal para culpar a la IA por el acto lesivo.

Deepfake: caso Brad Pitt

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

Este caso resulta emblemático y sienta un precedente del uso de la IA generativa para cometer actos que dañan a otras personas. Es el caso de una dama de 53 años de origen francés que fue víctima de una romance scam o estafa romántica en línea por medio del uso de IA.

Según De Dios (2025), la dama llamada Anne asumió tener una relación amorosa con el famoso actor Brad Pitt. Ella comenzó a recibir mensajes, imágenes o fotos del actor en donde este le declaraba su amor hasta el punto de proponerle matrimonio. Todo fue creado mediante IA o deepfakes.

A la víctima, dicha situación le costó 830 mil euros que le transfirió al presunto Brad Pitt, o, mejor dicho, a los cibercriminales o ingenieros sociales quienes le hicieron creer a ella que Brad Pitt estaba con una enfermedad terminal y, que, debido a su proceso de divorcio, tenía congelado su dinero, y por lo tanto no podía pagar el tratamiento. Y a pesar de que la víctima dudó en realizar los envíos de dinero, al final “mordió el anzuelo”.

Siguiendo la tesis de De Dios (2025), los estafadores habían investigado a la víctima, quien tuvo graves problemas de salud y pasaba por un proceso de divorcio, lo cual la colocaba en una situación de vulnerabilidad. Al final, ella se dio cuenta de la estafa cuando vio al actor en las noticias bien de salud y con su nueva pareja.

El caso precitado es un ejemplo claro de cómo la IA puede utilizarse en perjuicio de las personas cuando aquella cae en manos de ingenieros sociales, quienes investigan vulnerabilidades de las víctimas a través de redes sociales, como en este caso. En conclusión, le exposición imprudente de los usuarios de redes sociales, los hace más vulnerables a estos actos.

3. Sobre otros ciberdelitos realizados con IA

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

Existe un universo de ciberdelitos que con el tiempo han ido evolucionando, tendiendo el denominador común que son cometidos por medio o con la ayuda de las TIC, y claro, con el desarrollo de la IA o Inteligencia Artificial. A continuación, se abordarán algunos ciberdelitos que tienden a ser de los más discutidos dentro del campo de la ciberdelincuencia y que también pueden ocupar IA en su comisión.

3.1 Phishing

El denominado phishing o pesca informática, consiste en que los ciberdelincuentes envían mensajes dirigidos (spear phishing) o en masa (phishing), con el objetivo de obtener información sensible de los usuarios para afectarles su patrimonio u otro bien jurídico tutelado.

Según Maldonado Montenegro (2024) citando a Suastegui (2022), el phishing como ciberdelito se describe de la siguiente manera:

> Consiste en un ciberataque en el que los piratas informáticos engañan a los usuarios para que entreguen información confidencial, incluidas contraseñas, datos bancarios y CPF. Por lo general, este tipo de ciberdelito dirige al usuario a un sitio web idéntico; por ejemplo, a una sucursal bancaria real. En esta página falsa, que funciona como cebo, los piratas informáticos pescan datos de los usuarios (Suastegui, 2022) (p. 32).

Igualmente, en lo que corresponde a la comisión de phishing por medio del auge de la IA, Bravo (2024) colige:

> Según investigadores de seguridad de IA en ETH Zurich, el gran auge de ChatGPT se vio acompañado de un daño colateral muy peligroso: el enorme aumento de correos de phishing. La IA generativa se convirtió en el mejor aliado para diagramar formas de engañar a las personas para que estas revelen información sensible, ya sea para sacar un rédito económico o utilizarla para otras acciones maliciosas (pág. 5).

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

Es decir, en el caso de ChatGPT, los ciberdelincuentes encuentran una cantera de formas o procesos que les ayuda en la manera de aplicar tácticas de ingeniería social a las potenciales víctimas a través de los mensajes que se les remiten mediante phishing.
Incluso, se puede colegir que los ataques de phishing mediante el uso de IA pueden ser más eficientes que los realizados sin el uso de esta.

Ejemplo de ello es, lo que expresa Shea (2025) respecto al uso de IA para cometer phishing. Resulta que en el Black Hat USA 2021, la Agencia de Tecnología del Gobierno de Singapur realizó un experimento en el que el equipo de seguridad envió correos electrónicos simulados de phishing selectivo a usuarios internos. Algunos de estos correos fueron creados por personas, mientras que otros se generaron mediante la tecnología GPT-3 de OpenAI. Un número significativamente mayor de personas hizo clic en los enlaces de los correos electrónicos de phishing generados por IA que en los de los escritos por personas.

Finalmente, los ataques de phishing han mejorado debido al uso automatizado de la Inteligencia Artificial, que ha acumulado más estrategias de cómo llevar a cabo este tipo de ciberdelito, incluso con mayor eficiencia que aquellos que no dependen de la IA, según datos de investigación recopilados.

3.2 Doxing o Doxxing

Este ciberdelito consiste en recopilar y publicar información de personas o usuarios activos desde y en las redes sociales con el fin de extorsionar o intimidar al titular, o en su caso, crear noticias falsas de estos, Bravo (2024).

Según Bravo (2024), gracias a la IA, se pueden recopilar grandes cantidades de datos de Internet, incluidos datos personales, y así los cibercriminales pueden deducir, por ejemplo, dónde podría estar ubicada una persona en específico o su familia; o patrones de comportamiento de esta.

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

La regla es básica y simple, se está mucho más vulnerable y aumenta el riesgo de ser víctima de este tipo de prácticas en la medida en que se publica más información de carácter personal en internet, especialmente en las redes sociales. Por ello, entre menos una persona publique menor es el riesgo.

El sitio web Argentina.gob.ar (2025), establece que el doxxing consiste en recopilar y publicar información personal de otras, sin el consentimiento previo, con el objetivo de dañar su vida privada o profesional.

Asimismo, el precitado sitio web infiere respecto al doxxing que, la información que se obtiene de las personas que son afectadas, es recopilada de las redes sociales, de bases de datos robadas e incluso de la Deep web.

En conclusión, el doxxing es un tipo de ciberdelito basado en recopilar documentación o información personal sensible de las víctimas sin el consentimiento de estas, con el fin de dañar su reputación, mediante sextorsión, cometer ciberacoso o incluso cyberbullying.

3.3 Del Robo de Identidad

Del mismo modo, existe robo de identidad, el cual se relaciona con el precitado caso del famoso actor Brad Pitt, en donde se creó mediante herramientas de IA una imagen de este. Entonces, el robo de identidad es utilizar los datos personales de otro individuo, sin su consentimiento, y en su perjuicio, o de terceros.

Las actividades delictivas on line han aumentado, sin perjuicio del crecimiento que se dio durante la pandemia del Covid19. Pero, de igual forma, los fraudes informáticos, scams, phishing, entre otros, han tenido auge desde antes de la pandemia y a posteriori de ella. Y una de las formas más comunes para poder cometer scam en línea, es a través del robo de identidad que va de la mano con la creación de perfiles falsos.

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

La mejor manera en que puede aminorarse el riesgo de ser víctima de robo de identidad es la forma en que cada persona o usuario activo maneja su información personal en las redes sociales, es decir, entre menos información, sobre todo sensible se comparta, el riesgo debería disminuir.

Sin embargo, en redes sociales, los padres exponen hasta sus propios hijos menores de edad, a través del sharenting, lo cual se explicará a continuación.

3.4 Sharenting: el riesgo de compartir la vida privada en las redes sociales

Este acto denominado sharenting, proviene del vocablo en inglés share que significa compartir y parents o parenting (paternidad). Consiste en todas aquellas acciones en donde un usuario de red social comparte información privada o sensible, apareciendo y mostrando imágenes o vídeos con sus propios hijos, por ejemplo, fotos en lugares que ha visitado recientemente o lugares que frecuenta, entre otros aspectos.

De conformidad con Gatto et. al. (2024):

> Introduced in the Oxford English Dictionary in 2022 and now widespread throughout the world, “sharenting” defines the habit of sharing on social media photos of their children. The term comes from the union of share (to share) and parenting (to be parents). Steven Leckhart used this word for the first time in an article titled “The Facebook-Free Baby. Are you a mom or dad who’s guilty of ‘oversharing’? The cure may be to not share at all”. [Introducido en el Oxford English Dictionary en 2022 y ahora extendido en todo el mundo, el "sharenting" define el hábito de compartir en las redes sociales fotos de sus hijos. El término proviene de la unión de compartir (compartir) y crianza (ser padres). Steven Leckhart usó esta palabra por primera vez en un artículo titulado "El bebé libre de

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

> Facebook. ¿Eres una mamá o un papá que es culpable de 'compartir demasiado'? La cura puede ser no compartir en absoluto"] (p. 2).[2]

Según Chávez (2021), el sharenting es la acción o proceder por parte de los padres de un menor basada en compartir la vida de estos desde que nacen, su primera sonrisa, la primera vez que va solo al baño, el primer diente que se le cae, entre otros aspectos íntimos del impúber.

Asimismo, Chávez (2021), deduce que esta práctica no es un delito informático, pero sí se puede reputar como una costumbre que los padres creen que es inocua, sin embargo, el contenido compartido puede ser visto por pedófilos o personas que luego busquen o contacten a estos menores para cometer child grooming o cyberbullying, u otro acto ilícito como un secuestro extorsivo.

4. **Inteligencia Artificial: prevención de ciberdelitos**

La IA, a como se explicó, puede ser utilizada para la comisión de ciberdelitos ya que esta, en teoría, emula actos que podrían realizar las personas. Pero, asimismo, puede ser utilizada para la persecución y lucha en contra del cibercrimen. A continuación, se explicará sobre tales aspectos.

4.1 IA: defensa cibernética

Según el sitio web de la Universidad Nacional del Cuyo (2024), la Inteligencia Artificial o IA, también juega un papel importante en la defensa cibernética debido a la capacidad que esta tiene de analizar grandes cantidades de datos y con ello, prever comportamientos potencialmente maliciosos, otorgándoles a los expertos en ciberseguridad el conocimiento para luchar en contra de los ciberdelitos.

[2] Traducción propia del autor.

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

Zambrano Rendón (2024), en lo que respecta a los ataques basados o con la ayuda de la IA expresa lo siguiente:

> En la actualidad, la inteligencia artificial (IA) está experimentando un rápido avance y la frecuencia de los ataques cibernéticos sigue en aumento, por lo tanto, comprender cómo los agentes maliciosos emplean la IA para llevar a cabo sus ataques se ha convertido en una prioridad crítica. Mediante acciones como la exploración de los patrones emergentes, las técnicas y estrategias, se espera contribuir de manera significativa a la formulación de estrategias efectivas para contrarrestar y mitigar los ciberataques basados en la IA (p. 4).

Resulta que la escala de la IA cada vez es mayor y, en tal crecimiento, los riesgos atinentes a la ciberseguridad igualmente se han acrecentado. Anteriormente, se analizó cómo ChatGPT puede ser utilizado para desinformar o generar información que coadyuve a ciberdelincuentes. Ahora, desde enero de 2025 salió la denominada DeepSeek que es un Chatbot originario de China y potenciado por IA como el ChatGPT, OpenAI o Gemini (Ng & Drenon, 2025). Este brinda respuestas a las preguntas que se le formulan, aunque con mayor propensión a la conversación.

Por su parte, en palabras de Assalian (2025), esta nueva herramienta de IA está siendo utilizada para la generación de softwares maliciosos o malwares, o incluso puede crear dichos programas de forma autómata. Sin embargo, el desarrollo de esta herramienta es básicamente nueva, y tendrá que verse su crecimiento y asimilación por parte de la población.

Y en palabras de Pellejero Cuenca (2023), se explica la realidad de la IA respecto a la cibercriminalidad en estos días, de la siguiente forma:

> Como todos los avances tecnológicos destacables, este fenómeno también ha dado lugar a nuevas adaptaciones de comportamientos delictivos, planteando nuevos

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

> desafíos para la seguridad y la aplicación de la ley, cuya respuesta ha sido amoldarse a dicha tecnología disruptiva (p.2).

Amén de lo anterior, Pellejero Cuenca (2023), citando a Ortega et. al. (2021), plantea que al igual que el avance de la cibercriminalidad por medio de la IA, también existen mejoras en los sistemas de prevención e investigación criminal existentes, lo cual obliga a optimizar procedimientos como la utilización de sistemas radiofónicos que permiten una mejor coordinación grupal, entre otros aspectos.

4.2 IA: herramientas en la lucha contra el cibercrimen

Pellejero Cuenca (2023), citando a Quevedo (2017), aduce que, en España, en lo que respecta a la investigación penal tecnológica, hay una práctica que se basa en la obtención de direcciones IP e IMEI, identificación y conservación de datos, captación de conversaciones públicas, entre otros.

Asimismo, de conformidad con Pellejero Cuenca (2023) citando a Alonso (2021), existen otros sistemas, como el denominado VeriPol, herramienta de IA utilizada en España para detectar denuncias falsas.

En España existe el sistema de reconocimiento facial biométrico automático denominado Abis, que utiliza datos que almacenan los cuerpos de seguridad al realizar detenciones (Pellejero Cuenca, 2023).

Amén de todas las herramientas descritas, lo que no se sabe aún o no se tiene total certeza, son los límites a los cuales llegará la humanidad con el avance sostenido de la Inteligencia Artificial o IA, sea para bien o para mal. Igualmente, genera muchas interrogantes cómo el Derecho regulará estas nuevas herramientas tecnológicas basadas en IA, sobre todo en lo que respecta a la comisión de ciberdelitos, a como se analizó en el presente trabajo investigativo.

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

Conclusiones

Como respuesta a la pregunta de investigación, quedó claro que, la Inteligencia Artificial o IA, mediante los procesos descritos en esta investigación, ayuda en la comisión de ciertos ciberdelitos que afectan el honor, la intimidad, la privacidad y el patrimonio.

Los cibercriminales tienen en cierto grado, ventaja sobre las autoridades que luchan contra el ciberdelito porque viven en continua evolución, adecuándose a los cambios y aprovechándose de ellos, como es el caso del uso de la Inteligencia Artificial o IA.

La Inteligencia Artificial o IA no es necesariamente inicua o mala, a como pasa también con la tecnología en general o las TIC. Son las personas que la utilizan y que ponen en práctica los procesos acá analizados a quienes se les puede atribuir la culpabilidad o juicio de reproche por dichos actos ilícitos. La Inteligencia Artificial o IA, por consiguiente, no es sujeto de derecho.

La tecnología y en especial la IA, hasta el momento no se pueden reputar como personas o seres humanos, a pesar de que traten de realizar o emular actos humanos automatizados o entrenados.

La voluntad humana como tal, es humana no robótica, ni está adecuada o nace de un programa o algoritmo, y sin voluntad humana, no puede existir acción propiamente dicha en la comisión de un acto delictivo, por ende, un robot o una herramienta de IA, hasta el momento carecen de voluntad y, por lo tanto, de responsabilidad criminal.

Al final, toda la tecnología es creada, diseñada y desarrollada por seres humanos. La tecnología, por sí sola, no puede existir. Si esto llegase a pasar, en ese momento sí cambiarían todos los estándares o características jurídico-sociales que solamente se les atribuían a los seres humanos.

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

Por medio de IA, se pueden crear deepfakes, o, noticias falsas (fake news) que dañan o lesionan bienes jurídicos de terceros, porque el primero crea imágenes, vídeos y hasta la voz de otras personas para estafar o engañar a terceros, y la segunda, desinforma a través de redes sociales, y con ello, pueden distorsionar lo que en realidad ocurrió, crear caos y malas interpretaciones.

Se puede realizar doxxing y robo de identidad con ayuda de la IA ya que esta puede dar herramientas para la comisión de estos ciberdelitos. Igualmente, el sharenting analizado en el presente trabajo investigativo, también facilita la comisión de este tipo de ciberdelitos, u otros más graves como el child grooming, o secuestros extorsivos, al exponer a menores de edad en las redes sociales.

Existen herramientas de IA, como en España, las cuales se utilizan conforme a la Ley, para la investigación criminal o penal en ciertos delitos. Es decir, la Inteligencia Artificial o IA, también ayuda a investigar y esclarecer cibercrímenes o delitos comunes, según el caso.

Y, por último, se logró determinar de conformidad a los documentos investigados, que el phishing es de los ciberdelitos que está teniendo considerable crecimiento por el uso de la Inteligencia Artificial (IA), sin perjuicio de los otros ciberdelitos analizados en el presente trabajo investigativo. Al final, la recomendación principal es que, toda persona mayor de edad debe aprender a gestionar adecuadamente la información que publica sobre todo en redes sociales y, transmitir dicho conocimiento a sus hijos y adultos mayores, para educarse en estos temas y así, disminuir los riesgos que conlleva el fenómeno del cibercrimen.

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

Referencias

Assalian, M. (2025). *Inteligencia artificial utilizada para crear malware avanzado. Security Advisor*.

Bravo, C. (2024, junio 27). *Las 5 maneras en las que el cibercrimen utiliza la inteligencia artificial. Esset.*

Chávez, K. (2021). *Sharenting, riesgos por sobreexposición de los niños, niñas y adolescentes en redes sociales. Revista Pensamiento Penal.*

Cumpa González, L. (2012). *Lenguaje y comunicación digital. Comunife, 12,* 126–137.

De Dios, V. (2025). *Deepfakes y Brad Pitt. Informador.mx.*

Fundación Telefónica. (2013a). *Identidad digital: El nuevo usuario en el mundo digital.* Editorial Ariel.

Fundación Telefónica. (2013b). *Identidad digital: En nuevo usuario en el mundo digital* (1ª ed.). Editorial Ariel.

Gatto, A., et al. (2024). Sharenting: Hidden pitfalls of a new increasing trend – Suggestions on an appropriate use of social media. *Italian Journal of Pediatrics, 50*(15). https://doi.org/10.1186/s13052-024-01584-2

Gercke, M. (2014). *Comprensión del ciberdelito: Fenómenos, dificultades y respuesta jurídica.* ITU.

Gestión. (2016, junio 3). *Siete características para identificar a un ciberdelincuente. Gestión.*

La Universidad en Internet. (2024). *Deepfake: ¿Qué es y cómo detectarlo?* UNIR.

Maldonado-Montenegro, Ch. (2024). Análisis sobre la integración de la inteligencia artificial en la lucha contra la ciberdelincuencia en el Ecuador: Desafíos y perspectivas. *Revista Criminalidad, 66*(3), 27–44. https://doi.org/10.47741/17943108.660

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)

Miranda Gonçalves, R. (2024). Amenazas digitales: Estrategias efectivas para enfrentar y combatir el cibercrimen. *Novos Estudios Jurídicos, 29*(3), 791–820. https://doi.org/10.14210/nej.v29n1.p791-820

Ng, K., & Drenon, B. (2025, enero 25). *Qué tiene de especial DeepSeek, la nueva herramienta china de inteligencia artificial (y en qué se diferencia de ChatGPT o Gemini). BBC News.*

Pellejero Cuencia, D. (2023). *IA en la seguridad y delincuencia. Implicaciones político-criminales para el futuro. Universitat* Oberta de Catalunya.

Romeo Casabona, C., & Romero Martín, M. (2023). *Derecho penal, ciberseguridad, ciberdelitos e inteligencia artificial. Comares*.

Rosas, A. (2001). Kant, espíritus y noúmenos. *Ideas y Valores, 116.*

Ruiz, C. B., & Cortés Borrero, R. (2023). Los ciberdelitos y la ciberseguridad: Una cuestión de género. *Informática y Derecho, 13,* 73–84.

Sample, I. (2020). What are deepfakes and how can you spot them? *The Guardian.*

Sadoian, L. (2025, febrero 19). *Ciberdelito impulsado por IA: ¿Está su empresa preparada para defenderse? UpGuard.*

Shea, S. (2024, octubre 22). *Cómo la IA está haciendo que los ataques de phishing sean más peligrosos. TechTarget.*

Todesca, A. (2023). IA y fake news: Cuando lo real puede sucumbir a mentiras cada vez más inteligentes. *Palermo Business Review, 27,* 9–20.

Universidad Nacional del Cuyo. (2024). *El papel crucial de la inteligencia artificial en la defensa cibernética.* Uncuyo.

We Are Social. (2024). *Digital 2024. Global Overview Report.*

Zambrano Rendón, A. (2024). Impacto de la inteligencia artificial en los ciberataques. *Revista Sinapsis, 24*(1).

Volumen 2. Número 2. Julio - Diciembre 2025
ISSN: 3028-4546 (En línea)