Novos Estudos Jurídicos

[NEJ], vol. 29, n. 3, 2024

AMENAZAS DIGITALES: ESTRATEGIAS EFECTIVAS PARA ENFRENTAR Y COMBATIR EL CIBERCRIMEN*

Rubén Miranda Gonçalves
Universidad de Las Palmas de Gran Canaria, Las Palmas de Gran Canaria, España

Contextualización: el presente artículo analiza las amenazas digitales que surgen con el uso de la inteligencia artificial. Para ello, nos centraremos en cómo esta tecnología se está usando para perpetrar un variopinto de cibercrímenes como pueden ser el phishing automatizado, smishing, malware inteligente, robo de identidad, ciberacoso, entre otros. Estas amenazas plantean retos significativos para la seguridad digital a nivel global y afecta a individuos, empresas y gobiernos, lo que provoca importantes consecuencias económicas y sociales.

Objetivos: analizar las amenazas digitales derivadas del uso de la inteligencia artificial en el cibercrimen y considerar sus riesgos y consecuencias para proponer alguna estrategia para combatirlo.

Método: metodología basada en una combinación de análisis teórico y revisión bibliográfica.

Resultados: a través de esta investigación se proponen soluciones tecnológicas, normativas y educativas para enfrentar dichas amenazas. Se subraya la importancia de la cooperación internacional y el desarrollo de marcos éticos; por último, se resaltará la necesidad de concienciación pública y formación en ciberseguridad para disminuir los riesgos de ataques cibernéticos junto con la aplicación de otras tecnologías avanzadas como el *blockchain* en la protección de infraestructuras digitales.

Palabras clave: Inteligencia artificial; Cibercrimen; Phishing automatizado; Skimming digital; Seguridad digital.

* Este artículo se ha elaborado en el marco del proyecto de investigación "La manipulación informativa como problema de seguridad y de calidad democrática: descripción, consecuencias y respuestas". PID2021-125068OB-I00, concedido por el Ministerio de Ciencia e Innovación de España

AMEAÇAS DIGITAIS: ESTRATÉGIAS EFICAZES PARA ENFRENTAR E COMBATER O CIBERCRIME

Contextualização: O presente artigo analisa as ameaças digitais que surgem com o uso da inteligência artificial. Para isso, focamos em como essa tecnologia está sendo utilizada para perpetrar uma variedade de cibercrimes, como phishing automatizado, smishing, malware inteligente, roubo de identidade, cyberbullying, entre outros. Essas ameaças apresentam desafios significativos para a segurança digital em nível global, afetando indivíduos, empresas e governos, com consequências econômicas e sociais importantes.

Objetivo: Analisar as ameaças digitais decorrentes do uso da inteligência artificial no cibercrime, considerando seus riscos e consequências, e propor estratégias para combatê-las.

Método: Metodologia baseada em uma combinação de análise teórica e revisão bibliográfica.

Resultados: Por meio desta pesquisa, são propostas soluções tecnológicas, normativas e educacionais para enfrentar essas ameaças. Destaca-se a importância da cooperação internacional e do desenvolvimento de marcos éticos. Por fim, ressalta-se a necessidade de conscientização pública e formação em cibersegurança para reduzir os riscos de ataques cibernéticos, juntamente com a aplicação de outras tecnologias avançadas, como blockchain, na proteção de infraestruturas digitais.

Palavras-chave: Inteligência artificial; Cibercrime; Phishing automatizado; Skimming digital; Segurança digital.

DIGITAL THREATS: EFFECTIVE STRATEGIES TO FACE AND COMBAT CYBERCRIME

Contextualization: this article addresses the digital threats that arise with the use of artificial intelligence. To do so, we will focus on how this technology has been exploited to carry out a variety of cybercrimes such as automated phishing, smishing, intelligent malware, identity theft, cyberbullying, among others. These threats pose significant challenges to digital security globally, affecting individuals, businesses and governments, causing significant economic and social consequences.

Objectives: to analyze the digital threats derived from the use of artificial intelligence in cybercrime and to analyze its challenges, risks, consequences proposing a strategy to combat it.

Method: methodology based on a combination of theoretical analysis and literature review.

Results: through this research, technological, regulatory and educational solutions are proposed to address these threats. The importance of international cooperation and the development of ethical frameworks is underlined; finally, the need for public awareness and training in cybersecurity to decrease the risks of cyber attacks will be highlighted along with the application of other advanced technologies such as blockchain in the protection of digital infrastructures.

Keywords: Artificial intelligence; Cybercrime, Automated phishing; Skimming; Digital security.

INTRODUCCIÓN

En las últimas décadas, la inteligencia artificial ha irrumpido positivamente en campos muy variados como la medicina, la industria o la comunicación. La capacidad que presenta la IA para procesar grandes volúmenes de datos ha provocado una gran transformación en nuestras vidas[1]. No obstante, esos datos no solo son procesados sino que esa misma IA puede aprender de ellos e incluso tomar decisiones de forma autónoma. Esta habilidad ha permitido, sin duda alguna, numerosos avances y tampoco puede negarse que ha mejorado significativamente la eficiencia, la precisión y la capacidad de innovación en muchos sectores. Aun así, frente a esa visión positiva, debe observarse la otra cara de la moneda, ya que la IA también se nos presenta de forma negativa cuando se emplea con fines maliciosos, lo que genera nuevas y sofisticadas formas de cibercrimen que ponen en jaque a la seguridad digital.

Con la llegada de la IA, la complejidad y la efectividad del cibercrimen se ha ido potenciando de manera considerable y los ciberdelincuentes están utilizando la IA para optimizar sus acciones. Esto implica que son más difíciles de detectar e incluso de combatir, lo que está redefiniendo el mundo de la delincuencia cibernética. Con todo ello se está planteando una gran amenaza para la seguridad digital, pues no solo se ataca a los individuos sino que también se busca atacar a los gobiernos y sus instituciones.

La IA está teniendo un impacto significativo en el ámbito de la seguridad y, cada vez más, es muy común su empleo para desestabilizar infraestructuras críticas[2], lo que genera una disminución de la confianza en los sistemas digitales. En este sentido, es necesario estudiar cuáles son sus impactos y así poder valorar las consecuencias económicas, sociales y políticas del cibercrimen que viene siendo impulsado por la IA y elaborar estrategias defensivas mucho más efectivas.

En este contexto, hay que entender cuáles son los diferentes usos negativos de la IA y cuál es su aplicación en el cibercrimen, por lo que a lo largo de las siguientes líneas se proporcionará un análisis de cómo la IA se está utilizando para cometer actividades delictivas en internet y se analizarán cuáles son las principales técnicas que emplean los cibercriminales,

[1] Los agentes basados en conocimiento, (sistemas o entidades autónomas) mediante el uso de algoritmos, son capaces de manejar grandes volúmenes de información lógica. En este sentido, los agentes lógicos emplean el razonamiento para procesar tanto la información recibida como la adopción de decisiones y resolución de problemas en tiempo real. STUART, Russell; NORVIG, Peter. **Artificial Intelligence. A modern approach**. 2. ed. New Jersey: Prentice Hall, 2003.

[2] Por infraestructuras críticas ha de entenderse "el elemento, sistema o parte de este situado en los Estados miembros que es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar social y económico de la población y cuya perturbación o destrucción afectaría gravemente a un Estado miembro al no poder mantener esas funciones". Artículo 2 a) de la Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

por ejemplo, el *phishing* automatizado, el *smishing*, el *malware* inteligente, los ataques DDoS basados en inteligencia artificial, entre otros. Para concluir, también propondremos algunas estrategias de defensa contra el cibercrimen y se ofrecerán recomendaciones que refuercen la solidez de las estructuras digitales para garantizar que la privacidad de los datos personales esté a salvo en un mundo cada vez más digitalizado.

1. USOS MALICIOSOS DE LA IA Y SU APLICACIÓN EN EL CIBERCRIMEN

Como hemos defendido anteriormente la IA no sólo 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[3].

Como disciplina de la informática que se dedica al desarrollo de sistemas capaces de realizar tareas que, normalmente, requieren de la inteligencia humana como son el razonamiento, la percepción, el aprendizaje o la toma de decisiones, la inteligencia artificial ha ido evolucionando desde que allá por 1950 Alan Turing introdujese el concepto de máquinas inteligentes y propusiera el "Test de Turing" para determinar si una máquina podía exhibir un comportamiento inteligente que fuese indistinguible del de un ser humano o cuando en 1956 John McCarthy acuñó, por primera vez, el término inteligencia artificial[4].

No puede negarse que la inteligencia artificial ha revolucionado numerosos sectores, desde la medicina hasta las finanzas, y que también ofrece beneficios que parecían impensables hace tan solo unas décadas. Sin embargo, esta misma tecnología tiene un potencial oscuro que ha comenzado a manifestarse en formas cada vez más sofisticadas de cibercrimen. De lo anterior se desprende que la IA suele ser asumida como un instrumento, sin embargo, olvidan quienes así piensan el reduccionismo de ese planteamiento. Hay quienes defienden no solo la necesidad de comprender que la inteligencia va más allá de la robótica, sino también cómo y quiénes la emplean, la diseñan, o programan.

[3] BECERRIL GIL, Anahiby Anyel. Retos para la regulación jurídica de la Inteligencia Artificial en el ámbito de la Ciberseguridad. **Revista IUS**, v. 15, n. 48, p. 9-24, 2021. Disponible en: https://www.scielo.org.mx/scielo.php?pid=S1870-21472021000200009&script=sci_arttext

[4] MIRANDA GONÇALVES, Rubén. Inteligencia artificial y derechos humanos: una solución a los conflictos éticos y morales a través de una regulación normativa futura. In: MIRAUT MARTÍN, Laura; ZALUCKI, Mariusz (Editores); MIRANDA GONÇALVES, Rubén; PARTYK, Aleksandra (Coordinadores). **Artificial Intelligence and Human Rights**. Madrid: Dykinson, 2021, p. 49.

En este sentido, y de manera unilateral, no se podría entender la autonomía de la voluntad de las máquinas inteligentes en tanto en cuanto no hay que olvidar que la inteligencia, como cualidad ontológica y propia de la razón, resulta proyectable exclusivamente en el ser humano en su acepción biológica natural. Asimismo, no puede negarse la existencia de un salto cualitativo en los algoritmos que sustentan la IA, lo que significa que han mejorado sobremanera su capacidad de crear contenido y resolver problemas a través de estos algoritmos. Ahora es el algoritmo quien se configura como el pilar de la IA porque "cuanta más complejidad algorítmica, más capacidad predictiva, de ahí que todos los esfuerzos se centren en correlacionar infinidad de variables para acertar en las previsiones de futuro"[5]. Ante este escenario, la pregunta que debemos plantearnos no es otra que la de ¿cómo ha influido el aumento de la complejidad algorítmica en el desarrollo de la IA y qué efectos ha tenido en la creación de contenidos manipulados? Este sería el caso de la creación de un *deepfake*, un vídeo digitalmente manipulado de forma tan realista que parece mostrar a una persona diciendo o haciendo algo que, en realidad, nunca ocurrió[6].

De esta manera, la creación de *deepfakes*, imágenes, vídeos o incluso audios es usada para difamar, para cometer fraude o incluso para manipular información que, en varias ocasiones, es difundida a través de redes sociales que "permiten con suma facilidad que el receptor reenvíe el mensaje recibido"[7]. A mayor abundamiento, también se han venido desarrollando técnicas de IA que engañan a otros sistemas automatizados como pueden ser los sistemas de seguridad.

La IA, al igual que otras tecnologías disruptivas, presenta una naturaleza dual. Por un lado, su capacidad para automatizar procesos, mejorar la eficiencia y reducir costos tiene el potencial de generar avances significativos en diversas áreas de la vida humana; pero, por otro lado, la IA puede ser utilizada para perpetrar actos que van en contra de la ética y el derecho, especialmente en el contexto del cibercrimen. Esta naturaleza dual se traduce en que la IA no solo genera un impacto significativo en la dignidad de la persona humana como ocurre con los *deepfakes,* sino que también cuenta con un alcance geopolítico. Así lo advierte González cuando señala que "el hecho es que la aplicación ilegítima de la IA está cuestionando los preceptos éticos en el campo de la ideología y la política, perturbando la legitimidad de los

[5] LÓPEZ BARONI, Manuel Jesús. Las narrativas de la inteligencia artificial. **Revista de bioética y derecho**, n. 46, p. 5-28, 2019. p. 10Disponible en: https://scielo.isciii.es/scielo.php?pid=S1886-58872019000200002&script=sci_arttext.

[6] GARCÍA DEL POYO, Rafael. La seguridad jurídica en el entorno digital. **Revista de Estudios Jurídicos**, n. 13, p. 182-202, 2013. p. 104. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5255445.

[7] FERNÁNDEZ RODRÍGUEZ, José Julio. Aproximación crítica a la manipulación informativa: el ejemplo de las redes sociales. **Gladius et Scientia. Revista de Seguridad del CESEG**, n. 3, p. 1-23, 2021. p. 2. Disponible em: https://revistas.usc.gal/index.php/gladius/article/view/8909.

procesos democráticos"[8] Por lo tanto, si tenemos en cuenta tal afirmación, podemos asentir que los ciberataques en la fenomenología delictiva afectan a la seguridad e integridad personal, así como a la dignidad y al espíritu propio de las sociedades democráticas, permitiendo la manipulación de la opinión pública o la desinformación.

En este escenario, la moral asumiría dos importantes proyecciones; por un lado, la dimensión activa y, de otro lado, la dimensión pasiva. Así las cosas, "en la agencia moral nos encontramos con un agente que actúa motivado por una elección moral y un paciente que recibe los efectos de la acción. En este sentido, la agencia moral no solo concierne el mundo de los actos o acciones, sino también la percepción y observación de los mismos"[9]. Este dilema nos lleva a formular una discusión filosófica sobre la relación entre el poder del derecho y el poder tecnológico, sobre todo en la cuestión que estamos tratando y que nos afecta, como es el cibercrimen. No obstante, es primordial no descuidar que el derecho debe adaptarse a las nuevas realidades sociales y tecnológicas para mantener su relevancia y su eficacia.

El cibercrimen ha venido evolucionando de formas inimaginables, incluso antes de la aparición de la IA. Actualmente, los cibercriminales pueden utilizar IA para automatizar ataques, evadir la detección y maximizar el daño a sus objetivos pues, al final, "los ciberdelincuentes (enemigos), tienen todas las herramientas para hacer colapsar el mundo"[10]. Un ejemplo claro de ello son el *phishing* automatizado y personalizado, el *smishing*[11] o incluso el *skimming* digital[12]. La IA permite la creación de correos electrónicos de *phishing* altamente personalizados y muy difícil de detectar. Los algoritmos de aprendizaje automático pueden analizar grandes volúmenes de datos sobre sus víctimas y crear mensajes que imiten casi a la perfección las comunicaciones. Estos ataques de *phishing* han alcanzado un nuevo nivel de sofisticación muy elevado gracias a la automatización basada en IA, lo que dificulta su

[8] GONZÁLEZ ARENCIBIA, Mario; MARTÍNEZ CARDERO, Dagmaris. Dilemas éticos en el escenario de la inteligencia artificial. **Economía y sociedad**, v. 25, n. 57, p. 1-17, 2020. p. 3. Disponible en: https://www.scielo.sa.cr/scielo.php?pid=S2215-34032020000100093&script=sci_arttext.

[9] MONASTERIO ASTOBIZA, Aníbal. Ética para máquinas: similitudes y diferencias entre la moral artificial y la moral humana. **Dilemata. Revista Internacional de Éticas Aplicadas**, n. 30, p. 129-147, 2019. p. 131. Disponible en: https://dilemata.net/revista/index.php/dilemata/article/view/412000295.

[10] JIMÉNEZ BERNALES, Luis Alberto. El estado actual del cibercrimen en Perú y el derecho alemán. **Boletín Mexicano de Derecho Comparado**, v. 56, n. 167, p. 197-219, 2023. p. 204 Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=9529435.

[11] El *smishing*, según Martínez Santander et. al., es "la combinación de la palabra "Phishing" y "SMS" (…) un nuevo tipo de técnica de Phising que roba la información de un usuario, usando el servicio de mensajería de texto (SMS) de un teléfono móvil" MARTÍNEZ SANTANDER, Carlos José et. al. "Seguridad por capas frenar ataques de Smishing", *Dominio de las Ciencias*, v. 4, n. 1, 2018, p. 118.

[12] Según la Europol, se refiere al acto de robar información de tarjetas bancarias que se encuentra en plataformas de pago en sitios web de comercio electrónico. Los datos de la transacción son capturados durante el proceso de verificación de la compra en línea, sin que los usuarios se den cuenta de que algo fuera de lo normal está ocurriendo. Este tipo de fraude también es conocido como *web skimming, online card skimming, e-skimming, formjacking* o *Magecart*. EUROPOL https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/digital-skimming:es

detección y aumenta su efectividad. Todos estos ciberdelitos "se realizan utilizando las TIC, Internet y, claro, la inteligencia artificial"[13].

Esta cuestión se puede complicar todavía más cuando la legislación no resulta eficaz. El claro ejemplo es el hecho de que la creación y empleo de un perfil falso en Internet, en principio, no contradice ninguna normativa vigente y podría ser vista como una manifestación de la libertad de expresión. Esta práctica puede derivar en riesgos cuando se llevan a cabo malas intenciones. De esta manera, el perfil falso puede resultar un instrumento que permita llevar a cabo ataques de *phishing* en connivencia con la automatización de la IA. De este modo, la línea entre la libertad de expresión y el abuso de estas prácticas se vuelve difusa, reformulando la ética en su relación a cómo proteger los derechos individuales sin comprometer la seguridad en línea[14].

Estas y otras muchas herramientas que pueden ser empleadas en el ciberespacio permiten a los cibercriminales actuar con mayor eficacia y anonimato ya que utilizan tecnologías avanzadas que eluden las barreras de seguridad convencionales, un anonimato que "en realidad, constituye uno de sus más elementales y preciados derechos"[15]. Este escenario plantea desafíos importantes para el derecho penal, que debe adaptarse rápidamente a esta nueva realidad donde las fronteras físicas y digitales se diluyen, sancionando "no sólo la lesión de los bienes jurídicos sino también la puesta en peligro de los mismos"[16]. En este caso, la dificultad para identificar y procesar a los responsables en un entorno tan dinámico ha obligado a una reevaluación de los métodos tradicionales de investigación y enjuiciamiento.

Uno de los mayores desafíos en la lucha contra el cibercrimen es la detección temprana de estos ataques. Los cibercriminales están utilizando IA para desarrollar métodos más sofisticados que les permiten evadir los sistemas de detección tradicionales. Sin ir más lejos, en al ámbito financiero, estos crímenes representan "una amenaza latente que debería tener muy alertas a todas las organizaciones empresariales para prevenir y detectar posibles

[13] TAPIA SÁNCHEZ, Leónidas Salvador. Tecnología y derecho: una mirada al comercio electrónico, el cibercrimen y el soft law. **Ars Iuris Salmanticensis: AIS: revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología**, v. 10, n. 1, p. 199-226, 2022. p. 202.Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8484220.

[14] TEMPERINI, Marcelo GI; MACEDO, Maximiliano. La problemática de los perfiles falsos en Facebook y su relación con el Cibercrimen. **Simposio Argentino de Informática y Derecho (SID 2015) - JAIIO**, v. 4, p. 185-198, 2015. Disponible en: https://sedici.unlp.edu.ar/handle/10915/55608.

[15] SUÁREZ-MIRA RODRÍGUEZ, Carlos. Internet y Derecho penal: viejos y nuevos delitos. In: FERNÁNDEZ RODRÍGUEZ, José Julio; SANSÓ-RUBERT PASCUAL, Daniel (Directores). **Internet: um nuevo horizonte para la seguridade y la defensa**. Santiago de Compostela: Universidad de Santiago de Compostela, 2010. p. 124.

[16] MIRAUT MARTÍN, Laura. **La implicación del concepto de probabilidad en el derecho**. Murcia: Laborum Ediciones, 2023. p. 71

violaciones a su sistema de seguridad de la información"[17]. Aquí es donde entra en juego el derecho, pues enfrenta el desafío de regular una tecnología que es inherentemente ambigua y que, a su vez, tiene el potencial de ser beneficiosa o perjudicial, dependiendo de cómo se use, en tanto en cuanto, "si bien existen iniciativas a nivel europeo y estatal, por el momento no encontramos un soporte legal que incluya todo lo relativo a la inteligencia artificial"[18].

El problema se da cuando se trata la responsabilidad, porque a nuestro juicio es uno de los aspectos más complejos cuando se abordan los usos maliciosos de la inteligencia artificial, incluso en el cibercrimen. ¿Quién es el responsable cuando se comete un ilícito a través de la inteligencia artificial? Podríamos pensar que es el desarrollador del *software*, pero también podría serlo el usuario que lo implementa o, yendo al otro extremo, ¿podría exigírsele responsabilidad a la propia inteligencia artificial? Desde el punto de vista del derecho penal tradicional, la responsabilidad se le puede atribuir o bien a una persona física o a una persona jurídica que comete el ilícito. No obstante, con la llegada de la IA esta cuestión se complica todavía más, porque al final estamos hablando de un tipo de IA que puede actuar de forma autónoma y sin intervención directa por parte de un humano. Quizás es el momento de reevaluar los conceptos jurídicos tradicionales a la hora de atribuir la responsabilidad penal en el nuevo contexto de la IA e incluir nuevas categorías de responsabilidad adaptadas a la realidad actual.

Al igual que ocurrió con la evolución del derecho hacia la responsabilidad penal de las personas jurídicas, se hace más que necesario adoptar nuevas categorías de responsabilidad que puedan aplicarse a la IA, especialmente en los casos donde sus decisiones autónomas derivan en conductas socialmente significativas, como los daños a terceros[19]. Así lo defiende Morán cuando propone "la regulación de la IA como la próxima frontera regulatoria, abonado a su vez a su estudio jurídico, considerando que una IA al no estar permeada de la natural subjetividad humana, es un hecho, lógico, posible y probable que cualquier información negativa, abusiva, inadecuada, indeseable y hasta ilegal, en forma de conocimientos, le fuera proporcionada y programada para cometer delitos, lo que sería el primer elemento necesario para debatir sobre la probable determinación de responsabilidad

[17] CHÁVEZ-BRAVO, Juan; MALPARTIDA-MÁRQUEZ, Darwin; VILLACORTA-CAVERO, Armando; ORELLANO-ANTÚNEZ, Juan. La influencia de la automatización inteligente en la detección del cibercrimen financiero. **Boletín de Coyuntura**, n. 31, p. 26-33, 2021. p. 27. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8488976.

[18] HERNÁNDEZ GIMÉNEZ, María. Inteligencia artificial y derecho penal. **Actualidad jurídica iberoamericana**, fasc. 2, n. 10, p. 792-843, 2019. p. 837. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6978830.

[19] DE LA CUESTA AGUADO, Paz M. Inteligencia artificial y responsabilidad penal. **Revista penal México**, n. 16 y 17, p. 51-62, 2020. Disponible em: https://dialnet.unirioja.es/servlet/articulo?codigo=7675764.

de una IA en materia penal"[20].

Resulta destacable, sin embargo, cómo en el marco de la responsabilidad civil derivada del uso IA y de los seguros que responden subsidiariamente, ya se cuenta con una especie de "cultura de la reclamación" en las sociedades más desarrolladas. De hecho, se comprueba como cada vez son más personas las que reclaman la responsabilidad civil contra operadores que utilizan instrumentos algorítmicos como base para sus procesos de IA[21].

Para ello, creemos que debe instaurarse un nuevo marco normativo que equilibre esta IA con la seguridad implementando normativa transparente; de lo contrario no se podrá garantizar la confianza en la IA. Cuanto mayor regulada y clara sea esa responsabilidad, menos impunidad habrá en su uso pernicioso. En este sentido, "el derecho, igualmente, debe evolucionar hacia el ciberderecho o el derecho digital"[22]. Es evidente que esta normativa ha de ir más allá de los ordenamientos jurídicos internos, porque la cooperación internacional es condición *sine qua non* para facilitar la persecución de crímenes cometidos a través de la IA desde un país a otro. Solo aprobando una normativa común se podrá facilitar la persecución de estos delitos que atraviesan fronteras y que, sin ningún género de duda, se han convertido en crímenes transnacionales.

La colaboración internacional se ha vuelto esencial para combatir los crímenes facilitados por la IA dado que los ciberdelitos suelen cruzar fronteras sin dejar ningún tipo de rastro[23]. El Convenio de Budapest[24], por ejemplo, fue un esfuerzo notorio para armonizar las legislaciones y facilitar la cooperación entre países en la lucha contra la ciberdelincuencia, a través del cual se les brindó a los Estados parte "la herramienta para buscar la condena de todas las formas de ciberdelincuencia, con la intervención de mecanismos legales preestablecidos y políticas orientadas a prevenir, perseguir, sancionar y erradicar los

[20] MORÁN ESPINOSA, Alejandra. Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera? **Revista IUS**, v. 15, n. 48, p. 289-323, 2021. p. 304 Disponible en: https://www.scielo.org.mx/scielo.php?pid=S1870-21472021000200289&script=sci_arttext.

[21] TAPIA HERMIDA, Alberto Javier. La responsabilidad civil derivada del uso de la inteligencia artificial y su aseguramiento. **Revista Ibero-Latinoamericana de Seguros**, v. 30, n. 54, p. 107-146, 2020. p. 111. Disponible en: https://revistas.javeriana.edu.co/index.php/iberoseguros/article/view/33793.

[22] TAPIA SÁNCHEZ, Leónidas Salvador. Tecnología y derecho: una mirada al comercio electrónico, el cibercrimen y el soft law. **Ars Iuris Salmanticensis: AIS: revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología**, v. 10, n. 1, p. 199-226, 2022. p. 200. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8484220.

[23] MORÁN ESPINOSA, Alejandra. Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera? **Revista IUS**, v. 15, n. 48, p. 289-323, 2021. Disponible en: https://www.scielo.org.mx/scielo.php?pid=S1870-21472021000200289&script=sci_arttext.

[24] También conocido como el Convenio sobre Ciberdelincuencia. Vid: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-14221

delitos"[25]. Sin embargo, la rápida evolución de la tecnología supera con frecuencia el ritmo de la normativa, lo que genera lagunas y provoca la necesidad de poner en marcha nuevos marcos jurídicos que aborden no solo los aspectos técnicos, sino también los aspectos éticos de la IA. Los delitos que afectan a derechos fundamentales como el honor, la intimidad, la privacidad, entre otros, demandan soluciones más ágiles y flexibles capaces de adelantarse a las innovaciones delictivas que surgen en el ciberespacio.

Podría pensarse que con la regulación normativa de la IA ya estaría todo resuelto, pero esta regulación, tal y como hemos comentado *supra,* no solo debe limitarse a los aspectos legales, sino también debe tener muy en cuenta los aspectos éticos. En esta parte, la Filosofía del Derecho puede contribuir significativamente proporcionando un marco para la discusión de los valores o principios que deben guiar el desarrollo y el uso de la IA. Sin ir más lejos, el principio de autonomía, tan discutido en la ética médica, podría aplicarse perfectamente para garantizar que las decisiones automatizadas por la IA respetasen la autonomía de los individuos afectados. Igualmente, debe traerse a colación el principio de justicia, a través del cual se exija a la IA y a sus desarrolladores que no perpetúen y exacerben desigualdades o discriminaciones y que eviten brechas sociales.

Aunque la IA conlleva riesgos significativos cuando se usa con fines ilícitos o que puedan ocasionar daños a terceros atentando contra los derechos inherentes del ser humano, tampoco podemos olvidar que tiene un potencial inmenso para beneficiar a la sociedad. Es necesario que el marco jurídico evolucione para enfrentar todos estos desafíos, equilibrando la protección de los derechos humanos y los derechos fundamentales, sobre todo que la regulación sea multidimensional y no solo abarque aspectos legales, sino también éticos, algo lo suficientemente flexible para que se adapte a las rápidas evoluciones tecnológicas. De lo contrario, lo que se conseguirá es que el ciberespacio se convierta "en un nuevo lugar para la perpetración de distintos ataques a bienes jurídicos tan importantes como la intimidad, el honor, la propiedad, la libertad sexual y hasta la integridad física y la vida"[26].

Esta regulación deberá enfocarse en asegurar que la IA sea transparente, pues tiene un impacto considerable en los derechos individuales y colectivos de las personas. No es una cuestión que solo deba ser asumida por el legislador, sino que también creemos que debe implicar a la sociedad a la hora de crear un marco ético que guie en el uso responsable de la IA.

[25] ESTUARDO DUARTE, Carlos. Ciberdelincuencia: análisis del Convenio No. 85 de Budapest y el compromiso del Estado de Guatemala. **Revista Ciencia Multidisciplinaria CUNORI**, v. 5, n. 2, p. 111-118, 2021. p. 111 Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8873588.

[26] RAYÓN BALLESTEROS, María Concepción; GÓMEZ HERNÁNDEZ, José Antonio. Cibercrimen: particularidades en su investigación y enjuiciamiento. **Anuario Jurídico y Económico Escurialense**, n. 47, p. 209-234, 2014. p. 211. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4639646.

2. EL CIBERCRIMEN POTENCIADO POR LA IA: RETOS, RIESGOS Y CONSECUENCIAS

El impacto del cibercrimen potenciado por la inteligencia artificial es multifacético y afecta a diferentes esferas: desde lo individual hasta lo colectivo, y desde la economía hasta los derechos fundamentales de los ciudadanos. La IA ha impulsado al cibercrimen a un nuevo nivel de sofisticación, aumentando significativamente el daño potencial que pueden sufrir tanto las personas como las organizaciones[27].

El uso de tecnologías avanzadas ha transformado las capacidades de los sistemas de vigilancia, análisis de datos y la ciberseguridad. Asimismo, este progreso también ha revelado una serie de riesgos y vulneraciones en los derechos humanos, lo que ha venido generando preocupaciones sobre la ética y la protección legal en este ámbito. A medida que la IA se integra más profundamente en los sistemas de seguridad digital, es esencial que se entiendan tanto sus ventajas como los desafíos éticos que plantea[28] sobre todo, teniendo en cuenta el impacto que se ha producido en la seguridad digital, donde se ha generado un profundo cambio en la manera en que los sistemas de defensa, las empresas y los gobiernos gestionan la protección de sus datos y sus redes.

La evolución de los derechos humanos a lo largo de la historia ha demostrado que nuevas sensibilidades sociales y tecnologías pueden generar demandas de derechos de una nueva generación, especialmente en contextos como el actual, donde la tecnología avanza rápidamente[29]. Este tipo de riesgos éticos y también jurídicos relacionados con la IA no solo son teóricos, sino que están afectando directamente a los derechos humanos y a los derechos fundamentales de las personas. La inteligencia artificial no solo ha transformado la capacidad de defensa y ataque, sino que también ha generado nuevos riesgos éticos y legales que, como señala Ester Sánchez, pueden afectar directamente a los derechos fundamentales[30]. Ignacio Ara Pinilla reconoce, en este punto, al margen de la aparición de nuevos derechos, una

[27] AYERBE, Ana. La ciberseguridad y su relación con la inteligencia artificial. **Análisis del Real Instituto Elcano (ARI)**, n. 128, p. 1-8, 2020. Disponible en: https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/ari128-2020-ayerbe-ciberseguridad-y-su-relacion-con-inteligencia-artificial.pdf.

[28] FERNÁNDEZ MARTÍNEZ, Luis Felipe. Reflexiones sobre la ética y la era digital. **Cuadernos Fronterizos**, n. 61, p. 20-24, 2024. Disponible em: https://erevistas.uacj.mx/ojs/index.php/cuadfront/article/view/6532/8161.

[29] MIRAUT MARTÍN, Laura. **La formulación jurídica del libre desarrollo de la personalidad**. Madrid: Dykinson, 2023.

[30] ESTER SÁNCHEZ, Antonio Tirso. El desafío de la Inteligencia Artificial a la vigencia de los derechos fundamentales. **Cuadernos Electrónicos de Filosofía del Derecho**, n. 48, p. 111-139, 2023. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8962445.

decidida “alteración de sentido” de algunos de los derechos tradicionales[31].

En el ámbito de la seguridad digital, el empleo de la IA ha permitido desarrollar sistemas capaces de realizar análisis en tiempo real de una gran cantidad de datos, identificar patrones de comportamiento anómalos y detectar amenazas potenciales antes de que se materialicen. Tecnologías como el *machine learning* y el procesamiento del lenguaje natural, por ejemplo, permiten a los sistemas de ciberseguridad analizar millones de interacciones por segundo, lo que facilita detectar cualquier indicio de actividad sospechosa con gran precisión.

La creciente capacidad de la IA para procesar grandes volúmenes de datos y detectar patrones puede, en manos equivocadas, ser utilizada para la vigilancia masiva o la manipulación de información, lo que afectará gravemente a la privacidad y a la libertad de expresión de los ciudadanos. Esto lleva a una necesaria reflexión sobre los límites éticos y jurídicos que deben imponerse al desarrollo de estas tecnologías. Como señala González López, la protección de los derechos humanos en la era digital demanda la creación de un marco normativo que no sólo contemple los avances tecnológicos, sino también las garantías fundamentales, en especial el derecho a la privacidad y a la autodeterminación informativa[32]. Este marco normativo debe ser capaz de equilibrar el progreso tecnológico con la salvaguarda de derechos esenciales, asegurando que la IA no se convierta en una herramienta de control o represión. Asimismo, debe garantizar, como no puede ser de otra manera, el respeto a la dignidad humana en este contexto de cambio y evolución social[33].

Si nos detenemos en el ámbito económico, por ejemplo, la IA ha permitido a los ciberdelincuentes lanzar ataques más efectivos y difíciles de detectar, lo que ha ocasionado grandes pérdidas financieras para las personas y también para muchas empresas. Estas violaciones pueden causar daños económicos sustanciales y comprometer la estabilidad de las personas, empresas e instituciones gubernamentales o financieras.

Uno de los efectos más inmediatos de los ataques cibernéticos basados en IA es el robo de datos financieros y personales. Este tipo de ataque permite a los delincuentes acceder a información sensible como datos personales, cuentas bancarias o tarjetas de crédito, que luego utilizarán para cometer fraudes. Este tipo de fraude cibernético no solo tiene un impacto directo en las víctimas afectadas, sino que también puede generar una pérdida de confianza a gran escala en las instituciones financieras, lo que afectará negativamente a su reputación y

[31] ARA PINILLA, Ignacio. El difuso fundamento normativo de los derechos humanos. **Revista ESMAT**, n. 26, p. 285-302, 2023. p. 296

[32] GONZÁLEZ LÓPEZ, Édgar. Los derechos digitales fundamentales ¿es necesaria su reconfiguración en el ordenamiento jurídico? **Revista de Derecho Administrativo**, n. 20, p. 234-267, 2021. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8510534

[33] PECES-BARBA MARTÍNEZ, Gregorio. Sobre el fundamento de los derechos humanos un problema de Moral y Derecho. **Anales de la Cátedra Francisco Suárez**, n. 28, p. 193-208, 1988. Disponible en: https://revistaseug.ugr.es/index.php/acfs/article/view/12259/10152.

reduciría su base de clientes[34].

Cabe agregar que el daño de los ciberataques no se limita únicamente al robo de datos. En el ámbito empresarial también debe hacerse frente a gastos adicionales en ciberseguridad, auditorías y recuperación de esos mismos datos que fueron robados, lo que representa un costo económico significativo a largo plazo. Las instituciones financieras, por ejemplo, se ven obligadas a destinar más recursos para fortalecer sus defensas ante las crecientes amenazas impulsadas por la IA. Tal y como afirma[35], los ciberataques generan la necesidad de una revisión continua y mejora de los sistemas de seguridad en las empresas, lo que representa un aumento constante en los gastos operativos. Estos gastos adicionales pueden ser particularmente difíciles de afrontar para las pequeñas y medianas empresas, que a menudo carecen de los recursos financieros para implementar medidas de seguridad avanzadas.

Otro aspecto negativo relevante es el daño a la confianza del cliente. Cuando una empresa sufre un ciberataque, especialmente si implica el robo de datos personales o financieros, los clientes pierden confianza en la capacidad de la empresa para proteger su información. Esa pérdida de confianza en las instituciones financieras debido a los ataques cibernéticos puede tener consecuencias devastadoras a largo plazo, ya que los clientes pueden optar por trasladar sus negocios a otras instituciones que perciban como más seguras . Esta pérdida de clientes no sólo afectará a los ingresos inmediatos de la empresa, sino que también reducirá su cuota de mercado y su capacidad para competir.

En el contexto de los mercados financieros globales los ataques cibernéticos pueden generar una inestabilidad considerable. No hay duda de que "la influencia de la Inteligencia Artificial General en la economía va más allá del mercado laboral, el crecimiento económico o los ingresos fiscales"[36]. Las grandes instituciones financieras son clave para el funcionamiento de los mercados y los ciberataques que comprometen sus sistemas, lo que afecta negativamente a la confianza de los inversores y provocan fluctuaciones en los mercados bursátiles. Al final, en una economía globalizada como la actual los ataques cibernéticos pueden desencadenar una reacción en cadena que afecte tanto a las instituciones

[34] CHÁVEZ-BRAVO, Juan; MALPARTIDA-MÁRQUEZ, Darwin; VILLACORTA-CAVERO, Armando; ORELLANO-ANTÚNEZ, Juan. La influencia de la automatización inteligente en la detección del cibercrimen financiero. **Boletín de Coyuntura**, n. 31, p. 26-33, 2021. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8488976.

[35] BONILLA BONILLA, Erika Viviana. **Propuesta de mejoramiento continuo de la seguridad informática y de la información en las instituciones de educación superior**. Bogotá D.C.: Universidad Santo Tomás, 2019. Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/20824/2019erikabonilla.pdf?sequence=15.

[36] PABLO-MARTÍ, Federico. **La Inteligencia Artificial General y sus riesgos**. Perspectivas SCCS: Explorando el Futuro de la Economía, Educación y Sociedad, p. 1-5, s.f. Disponible en: http://sccs.web.uah.es/wp/wp-content/uploads/2024/05/P2401-La-AGI-y-sus-riesgos.pdf.

financieras como a otras industrias relacionadas, poniendo en riesgo la estabilidad económica mundial.

Finalmente, la interrupción de operaciones es otra consecuencia directa de los ciberataques. Los ataques de denegación de servicio (DDoS) impulsados por IA, por ejemplo, pueden dejar inoperativas las plataformas digitales de las empresas durante horas o incluso días, lo que provocará la pérdida de ingresos y la interrupción de los servicios a los clientes. En sectores como el comercio electrónico o la banca en línea, donde las transacciones y los servicios son altamente dependientes de la conectividad y la disponibilidad constante, estos ataques tendrán un impacto financiero significativo.

Sin una correcta seguridad digital, las repercusiones en el sector económico pueden ser nefastas no solo afectando a un nivel microeconómico o con las empresas enfrentándose a pérdidas directas y costos crecientes en ciberseguridad, sino también a un nivel macroeconómico, donde los mercados financieros sufrirán las consecuencias de la inestabilidad generada por esos ataques. Es necesario que las empresas inviertan en tecnologías avanzadas de defensa y que los gobiernos y las instituciones internacionales implementen normativa que fortalezca la ciberseguridad en todos los niveles. Los ciberataques, en particular los que involucran robo de datos, daños a la reputación y fraudes financieros, afectan la productividad y el desarrollo económico de las empresas y, por extensión, de los países que dependen de la economía digital. Este es el caso de España, en el que el sector de la ciberseguridad cuenta con una brecha entre la oferta de profesionales capacitados y la creciente demanda de expertos en ciberseguridad[37].

Además del ámbito económico, resulta de especial interés analizar cómo es el impacto en el ámbito social, puesto que el cibercrimen facilitado por la IA ha generado una falta de confianza en las plataformas digitales. El aumento de los ataques de *phishing* altamente personalizados y automatizados, así como el uso de *deepfakes* para la manipulación de información y el fraude, ha venido provocando que muchos usuarios desconfíen de la información en línea y de las interacciones digitales.

Si tenemos en cuenta que el cibercrimen no solo ataca bienes económicos, sino que también afecta al acceso a servicios esenciales que, en muchos casos, dependen de la tecnología, nos daremos cuenta de que el bienestar también se ve comprometido. Por ejemplo, sectores como la educación y la salud pueden verse gravemente afectados por ataques cibernéticos que interrumpan servicios y pongan en riesgo la seguridad de los datos de sus usuarios.

[37] PAYÁ SANTOS, Claudio; CREMADES GUISADO, Álvaro; DELGADO MORÁN, Juan José. El fenómeno de la ciberdelincuencia en España: la propuesta de la Universidad Nebrija en la capacitación de personal para la prevención y el tratamiento del ciberdelito. **Revista Policía y Seguridad Pública**, v. 1, año 7, p. 237-270, 2017. Disponible en: https://camjol.info/index.php/RPSP/article/view/4312.

En el caso en concreto de la educación, los cibercriminales pueden atacar infraestructuras digitales educativas accediendo a bases de datos que contengan información personal y académica de estudiantes, profesores o personal de administración y servicios. Una vez se obtenga dicha información, puede ser usada para robo de identidad o incluso para extorsión, poniendo en riesgo su privacidad e incluso interrumpiendo el funcionamiento de dichas plataformas educativas.

El sector de la salud también es un objetivo frecuente del cibercrimen, ya que los sistemas hospitalarios dependen cada vez más de la tecnología para gestionar bases de datos de pacientes, realizar diagnósticos y coordinar tratamientos. Los ciberataques a hospitales y a clínicas pueden acarrear consecuencias extremadamente perjudiciales. Un ataque que inutilice los sistemas de salud no solo va a comprometer la privacidad de los datos médicos (que son extremadamente sensibles), sino que también pondrá en peligro la vida de los pacientes. Otro ejemplo serían los ataques de *ransomware*[38] en hospitales, que pueden bloquear el acceso a historiales médicos, sistemas de monitorización de pacientes o dispositivos médicos conectados, lo que podría retrasar o interrumpir tratamientos urgentes[39]. En algunos casos, los cibercriminales han exigido grandes sumas de dinero para liberar estos sistemas, poniendo a las instituciones de salud en una situación de alto riesgo.

El impacto de los ciberataques a servicios esenciales va más allá de las interrupciones inmediatas. En el ámbito social, los ciudadanos pierden la confianza en la capacidad del gobierno y las instituciones para proteger los servicios básicos, lo que inevitablemente genera una inestabilidad social. Además, la interrupción prolongada de servicios como la electricidad o el agua tiene un efecto dominó en otras áreas, como la seguridad pública, la atención médica y la economía. En términos económicos, las interrupciones en infraestructuras críticas pueden causar pérdidas multimillonarias debido a la inactividad de las industrias, el costo de reparación de los sistemas afectados y el impacto en el comercio.

Analizada esta cuestión, podemos observar cómo la introducción de IA en el ámbito del cibercrimen plantea numerosos desafíos, no solo jurídicos sino también filosóficos. Anteriormente hacíamos referencia la autonomía, y es que con la llegada de la IA podemos comprobar cómo esta puede actuar de forma autónoma, por tanto, ¿quién es el responsable? Los ordenamientos jurídicos han de atajar muchas de las lagunas jurídicas existentes, pues no siempre existe legislación que regule todos los tipos de responsabilidad en los delitos que se cometen mediante IA.

[38] "Programa que secuestra la información guardada en el disco duro de la computadora o computadoras" (TAPIA, 2022, p. 216).

[39] Un ejemplo de ello fue el ataque informático a un hospital de Dusseldorf en 2020, en Alemania, o el ciberataque que sufrió el servicio irlandés de salud en 2021.

En este sentido, deben traerse de nuevo a colación las palabras de Tapia Sánchez, y es que el derecho ha de "evolucionar hacia el ciberderecho o el derecho digital, el cual dentro de sus ramas plantearía el derecho global digital internacional con el objetivo de crear un derecho originario contenido en tratados o convenios internacionales para regular y garantizar la seguridad jurídica, el tráfico de información, la información personal y la justicia en el actual mundo digital"[40].

Este mismo dilema nos enfrenta a una cuestión filosófica trascendental que es la siguiente: ¿cómo ha de regularse esa autonomía de la IA en el contexto de la delincuencia cibernética? Un enfoque posible podría ser atribuir la responsabilidad a las personas o entidades que desarrollan y operan los sistemas de IA. Sin embargo, esto tampoco resolvería el problema de los sistemas que operan de manera completamente autónoma y sin intervención directa de los desarrolladores o los usuarios en el momento de cometer el delito. Igual resultaría necesario crear nuevas categorías jurídicas como la responsabilidad penal de los sistemas autónomos (actualmente no es posible imputar responsabilidad penal a un sistema de IA), o reforzar la responsabilidad indirecta de los desarrolladores y operadores de los sistemas.

Lo que está claro es que los delitos cibernéticos facilitan la perpetración de actos ilícitos a nivel transnacional y eso requiere una cooperación internacional más sólida para perseguirlos. Tal y como afirma García del Poyo[41], la naturaleza global de Internet complica la aplicación del derecho, ya que la normativa es local y no siempre está alineada entre diferentes jurisdicciones. Por un lado, el principio de autonomía podría aplicarse aquí para garantizar que las decisiones automatizadas de los sistemas de IA respeten los derechos y la dignidad de los individuos afectados. Por otro lado, también el principio de justicia exigiría que la IA no perpetúe ni exacerbe desigualdades o injusticias, por ejemplo, a través de decisiones discriminatorias o la manipulación de información.

En todo caso, entre las posibles estrategias y/o soluciones, teniendo en cuenta todo lo anterior, es primordial el desarrollo de estrategias de defensa que combinen soluciones tecnológicas, normativas y éticas. En primer lugar, las empresas y los gobiernos deben invertir en tecnologías basadas en IA para combatir los ciberataques. Como apunta Guaña-Moya[42], es fundamental aplicar estándares internacionales de seguridad informática

[40] TAPIA SÁNCHEZ, Leónidas Salvador. Tecnología y derecho: una mirada al comercio electrónico, el cibercrimen y el soft law. **Ars Iuris Salmanticensis: AIS: revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología**, v. 10, n. 1, p. 199-226, 2022. p. 200. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8484220.

[41] GARCÍA DEL POYO, Rafael. La seguridad jurídica en el entorno digital. **Revista de Estudios Jurídicos**, n. 13, p. 182-202, 2013. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5255445.

[42] GUAÑA-MOYA, Javier. La importancia de la seguridad informática en la educación digital: retos y soluciones. **RECIMUNDO: Revista Científica Mundo de la Investigación y el Conocimiento**, v. 7, n. 1, p. 609-616, 2023. p. 614. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8977055.

como la norma ISO/IEC 27002:2013[43], para asegurar que las infraestructuras digitales estén protegidas contra las amenazas cibernéticas. Estos marcos normativos son esenciales para que las organizaciones mantengan la confidencialidad, integridad y disponibilidad de la información.

Asimismo, el derecho debe adaptarse a las nuevas realidades del cibercrimen mediante el desarrollo de un marco normativo claro que regule el uso de la IA y asigne responsabilidades de manera justa y efectiva. Es necesario que los sistemas legales reconozcan el papel central que la IA está jugando en la perpetración de delitos y que se establezcan mecanismos de rendición de cuentas para los desarrolladores y operadores de estas tecnologías. Como señala García del Poyo[44], es imprescindible que el marco regulador contemple la protección de datos y las garantías jurídicas necesarias para evitar que la información crítica de las empresas sea vulnerada.

Creemos también que la cooperación internacional es clave para combatir el cibercrimen transnacional. El Convenio de Budapest y otras iniciativas internacionales deben actualizarse para abordar las nuevas formas de delincuencia facilitadas por la IA, permitiendo una colaboración más ágil entre los Estados. Las brechas normativas entre diferentes jurisdicciones facilitan la impunidad de los ciberdelincuentes, lo que subraya la importancia de un marco regulatorio común que facilite la persecución y enjuiciamiento de estos crímenes. Sin una cooperación internacional efectiva, los esfuerzos individuales de los países serán insuficientes para enfrentar la magnitud del cibercrimen global porque, como es sabido y así lo afirma Merino, el "fenómeno de la criminalidad no es estático, varía constantemente en virtud de la realidad jurídica, sociológica, política, económica, tecnológica, etc.; siendo necesario un sistema regulatorio que tutele bienes jurídicos de relevancia"[45].

Las soluciones éticas han de integrarse en el diseño de los sistemas de IA y los desarrolladores deben seguir principios de diseño que garanticen que los sistemas sean transparentes y que sus decisiones puedan ser auditadas. La implementación de un enfoque ético en el desarrollo de la IA puede ayudar a prevenir el uso indebido de estas tecnologías y reducir el riesgo de que se utilicen para fines maliciosos. Este enfoque ético debe involucrar no solo a los legisladores, sino también a la sociedad en general con el fin de establecer un marco que proteja los derechos fundamentales en un entorno cada vez más impulsado por la

[43] Se encarga de ayudar a las organizaciones a establecer, implementar, mantener y mejorar la gestión de la seguridad de la información, proporcionando un conjunto de mejores prácticas para la gestión de la seguridad de la información.

[44] GARCÍA DEL POYO, Rafael. La seguridad jurídica en el entorno digital. **Revista de Estudios Jurídicos**, n. 13, p. 182-202, 2013. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5255445.

[45] MERINO AJILA, Francisco Javier. Evolución internacional de la legislación sobre ciberdelincuencia tras el Convenio de Budapest. **Ciencia Latina: Revista Multidisciplinar**, v. 8, n. 3, p. 3654-3671, 2024. p. 3666. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=9610593.

tecnología.

Este entorno digital no debe ser una caja negra impenetrable; es decir, los algoritmos y procesos de toma de decisiones que lo rodean deben ser comprensibles para los humanos. Como señala García del Poyo[46], la transparencia permite que los usuarios y los reguladores auditen las decisiones automatizadas, lo que es necesario para evitar posibles discriminaciones o sesgos algorítmicos. Un enfoque de diseño ético no solo debe incluir esta transparencia, sino también la posibilidad de rectificar decisiones que puedan ser incorrectas o perjudiciales.

Dado que los sistemas de IA pueden tomar decisiones autónomas, es fundamental que los desarrolladores y operadores de estos sistemas asuman la responsabilidad de los resultados que generan. Esto significa que debe existir un marco que permita identificar quién es el responsable cuando una IA comete un error o toma una decisión perjudicial, pues la capacidad de decisión del agente puede verse potenciada, tal y como afirma de La Cuesta[47], lo que exigiría profundizar en los modelos de responsabilidad para así prever cuáles pueden ser los posibles daños. Sin una clara asignación de responsabilidades, los riesgos de uso malicioso de la IA aumentan significativamente, ya que los desarrolladores o las entidades que utilizan estos sistemas pueden intentar eludir sus responsabilidades legales o éticas.

Por tanto, de todo lo anterior se deduce que la creación de un enfoque ético sólido para la IA no puede recaer exclusivamente en los desarrolladores de tecnología. El legislador también juega un papel muy relevante, puesto que debe establecer marcos normativos que guíen el desarrollo y uso de la IA. Esto incluye la aprobación de leyes que protejan verdaderamente los derechos fundamentales de las personas como el derecho a la privacidad, el honor, la intimidad personal y familiar, la protección contra la discriminación, entre otros. El desarrollo de la IA ha de alinearse con los valores sociales y reflejar las preocupaciones éticas de la población. Esto incluye garantizar que las tecnologías no exacerben las desigualdades existentes ni perpetúen discriminaciones.

3. ESTRATEGIAS PARA COMBATIR EL CIBERCRIMEN EN LA ERA DE LA IA

A raíz de los avances que se han venido produciendo en la inteligencia artificial, el cibercrimen ha aumentado, lo que ha provocado un cambio en la seguridad digital. Esta evolución no solo ha facilitado la detección y prevención de amenazas, sino que, como ya comentamos anteriormente, ha permitido a los ciberdelincuentes perfeccionar sus ataques.

[46] GARCÍA DEL POYO, Rafael. La seguridad jurídica en el entorno digital. **Revista de Estudios Jurídicos**, n. 13, p. 182-202, 2013. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5255445.

[47] DE LA CUESTA AGUADO, Paz M. Inteligencia artificial y responsabilidad penal. **Revista penal México**, n. 16 y 17, p. 51-62, 2020. Disponible em: https://dialnet.unirioja.es/servlet/articulo?codigo=7675764.

La IA ha posibilitado tanto a defensores como atacantes acceder a tecnologías de *machine learning* y automatización avanzada, lo que ha incrementado la rapidez, precisión y escala de los ciberataques. En este contexto, los ataques automatizados, como los perpetrados mediante *bots* y el uso de *deepfakes*, plantean grandes desafíos a la ciberseguridad que, por otro lado, requieren soluciones innovadoras y una cooperación global para poder mitigarlos. Además, como señala la profesora Verdugo Guzmán, la IA bien utilizada puede actuar como una barrera protectora en el ciberespacio, pero su mal uso es una amenaza directa para los derechos humanos[48].

A nuestro juicio, el uso de IA y *machine learning* en la ciberseguridad ha permitido avances significativos en la detección de patrones sospechosos y en la identificación de amenazas, donde en muchos casos los algoritmos se han adaptado a las nuevas tácticas de los ciberdelincuentes. Según Arantza León Camino, la implementación de sistemas de aprendizaje automático ha mejorado la capacidad de predecir y prevenir ataques cibernéticos, lo que resulta muy relevante en sectores críticos como el financiero y el sanitario[49].

El uso de tecnologías como *blockchain* ha transformado radicalmente la seguridad digital, especialmente en sectores como el financiero, aunque también en el sanitario, en donde la confianza en la integridad de las transacciones es imprescindible. A través de *blockchain* es posible crear registros descentralizados, inmutables y transparentes, lo que dificulta significativamente la manipulación de datos. Este sistema respalda que las transacciones sean verificables por todas las partes involucradas, eliminando la necesidad de intermediarios. Desde varios sectores se ha defendido el **uso de la tecnología *blockchain*** y las ventajas que desprende sobre todo en lo que a **seguridad** y **transparencia se refiere**, especialmente en sectores como las finanzas. Para avalar su eficacia resulta imprescindible contar con dos aspectos fundamentales: por un lado, la disponibilidad y, de otro lado, la persistencia.

La disponibilidad que se defiende es la que asegura una transacción legítima y que esta sea añadida a la cadena de bloques sin sufrir una denegación de servicio (DoS), incluso cuando algunos nodos corruptos intenten bloquear el proceso. De esta manera, se certifica que el sistema funcione de manera estable y no se vea comprometido por actores malintencionados. En la misma línea de reconocimiento, la persistencia avala que una vez una transacción se ha considerado estable por un nodo, los demás nodos podrán validar la transacción. Desde luego, para asegurar que los datos almacenados en la *blockchain* no

[48] VERDUGO GUZMÁN, Silva. **Ciberespacio, Metaverso y nuevos delitos que gravitan sobre los derechos humanos**. Valencia: Tirant lo Blanch, 2023

[49] LEÓN CAMINO, Arantza. **El agente encubierto virtual**. Tesis doctoral, Universidad Carlos III de Madrid, 2022. Disponible en: https://e-archivo.uc3m.es/rest/api/core/bitstreams/9350c3b3-b6d1-4cd0-aaae-7fc89480472a/content.

puedan ser alterados o manipulados una vez registrados, estos aspectos deben tenerse en consideración para acreditar la confianza en la integridad del sistema[50]. Sólo de esta manera se podría alcanzar que el *blockchain* se configure en una herramienta que tenga como objetivo la mejora en la eficiencia de los procesos que requieren transparencia y seguridad. Además, su implementación es fundamental en la prevención de fraudes y mejora considerablemente la transparencia[51], ya que cualquier intento de alteración es inmediatamente detectable a través del sistema distribuido de nodos. La criptografía avanzada también desempeña un papel esencial, no solo en el comercio electrónico, sino en la protección de comunicaciones sensibles como la transmisión de datos médicos, financieros o gubernamentales. Estas tecnologías permiten que la información confidencial viaje cifrada y solo sea accesible por el destinatario previsto, lo que refuerza la privacidad y la integridad de los datos.

Tal y como hemos defendido en otras ocasiones, aunque la IA ha demostrado ser una herramienta poderosa en la lucha contra el cibercrimen, su uso plantea desafíos éticos importantes que deben ser abordados mediante un marco regulatorio claro[52] como son, por ejemplo, la privacidad y la protección de datos, la transparencia y rendición de cuentas, discriminación, etc. No puede negarse, como bien apunta Silvia Verdugo que, utilizada de forma correcta, puede ser una herramienta esencial para detectar amenazas y prevenir delitos en el ciberespacio[53]. Sin embargo, el mal uso de estas tecnologías, como en el caso de los *deepfakes* o los ataques automatizados, representa un gran desafío para la protección de los derechos humanos[54], porque se corre el riesgo de violar la privacidad, manipular a las personas o promover ataques automatizados, entre otros.

Partiendo de la base de que el cibercrimen no conoce fronteras, se requiere una colaboración internacional efectiva. Tanto el Convenio de Budapest sobre Cibercrimen como el Reglamento General de Protección de Datos o más recientemente el Reglamento europeo de inteligencia artificial son fundamentales para la cooperación global en la persecución de estos delitos, aunque no son suficientes. Asimismo, la cooperación entre los Estados es imprescindible para combatir los delitos en el ciberespacio, por lo que la naturaleza

[50] DOLADER RETAMAL, Carlos; BEL ROIG, Joan; MUÑOZ TAPIA, José Luis. La blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas. **Economía industrial**, n. 405, p. 33-40, 2017. Disponible em: https://dialnet.unirioja.es/servlet/articulo?codigo=6207510.

[51] MIRANDA GONÇALVES, Rubén; MOREIRA DOMINGOS, Isabela. Gobernanza blockchain: tecnología disruptiva para el control de la corrupción en la salud pública. **Revista Jurídica UNICURITIBA**, v. 4, n. 66, p. 31-49, 2021. Disponible en: http://hdl.handle.net/10553/113785.

[52] MIRANDA GONÇALVES, Rubén. Ethics, Technology and Rights: challenges to justiciability in the digital environment. **Legal and administrative studies**, v. 29, n. 2, p. 61-84, 2023. Disponible en: https://www.upit.ro/_document/304243/jlas_2_2023.pdf.

[53] VERDUGO GUZMÁN, Silva. **Ciberespacio, Metaverso y nuevos delitos que gravitan sobre los derechos humanos**. Valencia: Tirant lo Blanch, 2023

[54] VERDUGO GUZMÁN, Silva. **Ciberespacio, Metaverso y nuevos delitos que gravitan sobre los derechos humanos**. Valencia: Tirant lo Blanch, 2023

de estos crímenes exige una respuesta coordinada y eficiente[55]. Con todo, es un hecho que las normativas actuales son insuficientes para abordar las nuevas formas de delincuencia digital y que implican el uso de tecnologías avanzadas como la inteligencia artificial.

En este sentido, es imprescindible que los marcos normativos internacionales se actualicen para incluir disposiciones sobre el uso de IA en la seguridad digital, tal como sostiene Verdugo, pues la regulación de la IA en el ciberespacio debe centrarse en la protección de los derechos humanos, asegurando así que estas tecnologías no sean utilizadas para fines ilícitos[56]. Esta afirmación, sin duda alguna, refuerza la necesidad de armonizar las normativas entre diferentes jurisdicciones para garantizar una verdadera persecución efectiva del cibercrimen.

En un contexto global como el que nos encontramos, la falta de armonización normativa sigue siendo un obstáculo muy importante puesto que, como nos advierte Pérez Luño, el avance acelerado de la IA y el impacto que deriva de sus posibles acciones (ya sean o no lícitas) dificultan de manera considerable el proceso de definir y clasificar a fenomenología delictiva en el espacio digital[57]. Asimismo, sostiene el autor que la complejidad que implica todo lo que deriva del espacio digital en su relación con la ciberdelincuencia, asume una nueva forma de entender los bienes jurídicos y cómo se deben proteger. Paralelamente, además de contar con una variabilidad de conductas ilícitas como el *hacking*, el *phishing*, el fraude cibernético, la suplantación de identidad, que ya hemos defendido, se le suma la falta de regulación eficaz. De tal forma, se defiende en este sentido, la necesidad de no escatimar en esfuerzos en una cooperación entre los Estados. Sin una cooperación internacional efectiva y sin un marco normativo armonizado, la lucha contra el cibercrimen seguirá siendo fragmentada e ineficiente. Por ello, se hace necesario que los países adopten un enfoque común que permita la extradición de ciberdelincuentes y la colaboración en investigaciones internacionales.

El diseño y uso de la inteligencia artificial en el ciberespacio ha de alinearse con los principios éticos fundamentales para garantizar que se protejan los derechos humanos y evitar resultados discriminatorios. Los algoritmos, cuando no son transparentes o explicables, pueden perpetuar sesgos existentes y generar decisiones injustas, afectando desproporcionadamente a minorías o grupos vulnerables.

La necesidad de algoritmos explicables, como propone Tim Miller en su estudio sobre IA, permite a los usuarios entender cómo se toman las decisiones automatizadas, lo que

[55] VERDUGO GUZMÁN, Silva. **Ciberespacio, Metaverso y nuevos delitos que gravitan sobre los derechos humanos**. Valencia: Tirant lo Blanch, 2023

[56] VERDUGO GUZMÁN, Silva. **Ciberespacio, Metaverso y nuevos delitos que gravitan sobre los derechos humanos**. Valencia: Tirant lo Blanch, 2023

[57] PÉREZ LUÑO, Antonio-Enrique. **Manual de Informática y derecho**. Barcelona: Ariel, 1996.

facilita la responsabilidad y la rendición de cuentas. Esta transparencia es medular para evitar la discriminación y asegurar que las decisiones automatizadas se ajusten a los principios de justicia y equidad, tan necesarios en un entorno digital cada vez más dominado por la inteligencia artificial. En caso contrario, perjudicará a ciertos grupos de personas, por ejemplo, tomando decisiones que afecten de manera desproporcionada a minorías o grupos vulnerables. Para evitarlo, Tim Miller propone recurrir a los algoritmos explicables, es decir, algoritmos que permiten a los usuarios entender cómo se toman las decisiones automatizadas y que garanticen que estas decisiones no son arbitrarias ni discriminatorias[58].

Creemos que una de las áreas más importantes, pero a menudo descuidadas, en la lucha contra el cibercrimen es la educación y concienciación de los usuarios. Los ataques como el *phishing, smishing, skimming* digital o el *ransomware* a los que anteriormente nos referimos, suelen aprovechar la falta de conocimiento de los usuarios sobre las prácticas de seguridad digital. La educación de los usuarios será fundamental para mitigar los riesgos del cibercrimen, ya que la mayoría de los ataques dependen de la vulnerabilidad humana y se cometen aprovechándose de alguna debilidad informática y la ingenuidad de los usuarios[59] quienes, en la mayoría de las ocasiones, son víctimas de estos ataques debido a la falta de conocimiento o porque emplean inadecuadamente los dispositivos o servicios de internet[60]. Para ello, se recomienda lo que algunos han denominado como "ciberhigiene", es decir, "sencillas prácticas que nos ayudarán a evitar ser víctimas de los ciberdelincuentes si las cumplimos en nuestro día a día"[61]. Entre estos hábitos, por ejemplo, estaría la actualización constante de software, el uso de contraseñas seguras y la autenticación de dos factores, debe ser promovida entre los usuarios para mitigar estos riesgos. No obstante, más allá de la formación puntual, también se requiere la creación de una cultura de ciberseguridad a nivel organizacional.

Otra posible alternativa son los programas de capacitación en ciberseguridad para ayudar a los empleados y al público a reconocer las señales de alerta de posibles ataques y adoptar medidas preventivas. Además, las campañas de concienciación pública, promovidas por gobiernos y organizaciones internacionales, son fundamentales para educar a los

[58] MILLER, Tim. Explanation in artificial intelligence: insights from the social sciences. **Artificial Intelligence**, v. 267, p. 1-38, 2019. Disponible en: https://www.sciencedirect.com/science/article/pii/S0004370218305988.

[59] MIRÓ LLINARES, Fernando. La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing. **Revista Electrónica de Ciencia Penal y Criminología**, n. 15, p. 1-56, 2013. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4407809.

[60] ÁVILA NIÑO, Fredy Yesid; RINCÓN NÚÑEZ, Paola Maritza. Inclusión de la formación en prevención y atención de delitos informáticos en la educación policial. **Revista educación**, v. 42, n. 2, p. 1-28, 2023. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=9392396.

[61] INSTITUTO NACIONAL DE CIBERSEGURIDAD. **Pongamos en práctica la ciberhigiene**. Página web. Disponible en: https://www.incibe.es/ciudadania/blog/pongamos-en-practica-la-ciberhigiene.

ciudadanos sobre los riesgos del cibercrimen y las prácticas recomendadas para proteger su información personal.

En este sentido, es necesario que las organizaciones inviertan en la formación continua de sus empleados, especialmente en sectores tan críticos como el financiero y el sanitario, donde los ataques cibernéticos pueden tener consecuencias muy graves. La creación de una cultura de ciberseguridad dentro de las organizaciones es clave para garantizar que todos los empleados comprendan la importancia de proteger la información y los sistemas críticos. Con una buena capacitación de los usuarios, se reforzará la protección frente a amenazas y se permitirá una mejor respuesta a cualquier incidente que se plantee.

Se observa como en esta nueva era de inteligencia artificial la lucha contra el cibercrimen requiere un enfoque en el cual deben combinarse la tecnología avanzada, la cooperación internacional, la regulación ética y, por supuesto, la educación. En este sentido, la educación y concienciación de los usuarios sigue siendo uno de los pilares más importantes en la defensa contra el cibercrimen. La inversión en programas de capacitación y campañas de sensibilización pública puede reducir significativamente el número de ataques exitosos al aumentar la capacidad de los usuarios para identificar y responder a las amenazas. Al final, solo a través de una colaboración global y un enfoque ético en el desarrollo de la IA se podrá mitigar eficazmente el impacto del cibercrimen en nuestra sociedad, sin dejar de lado, como se ha dicho, la formación y concienciación de los ciudadanos que, en última instancia, somos el "eslabón más débil de la cadena de la seguridad"[62] y no estamos exentos de ser manipulados por quienes buscan obtener beneficios a costa de nuestras debilidades.

CONSIDERACIONES FINALES

Llegados al final de este artículo, se concluye que la IA ha transformado profundamente la forma con la que interactuamos con la tecnología, aportando innumerables beneficios en sectores como la medicina, la industria y la comunicación. Sin embargo, este avance también ha traído consigo una cara oscura: la utilización de la IA para fines maliciosos a través del cibercrimen. A medida que la IA se integra más profundamente en los sistemas tecnológicos, los ciberdelincuentes han comenzado a aprovechar su poder para llevar a cabo ataques cada vez más sofisticados, planteando nuevos desafíos para la seguridad digital.

De todo lo anterior se desprende que uno de los principales puntos a destacar es la dualidad de la IA. Si bien esta tecnología ha permitido la automatización de procesos y la mejora en la eficiencia de numerosos sectores, también ha sido utilizada para amplificar el

[62] SÁNCHEZ VERA, Fulgencio; MARTÍNEZ GUIRAO, Javier Eloy; TÉLLEZ INFANTES, Anastasia. La seguridad en el ciberespacio desde una perspectiva sociocultural. **Methaodos. Revista de ciencias sociales**, v. 10, n. 2, p. 243-258, 2022. p. 244. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8634381.

impacto de ataques cibernéticos. El *phishing* automatizado y personalizado, los *deepfakes* y el *malware* inteligente son algunos ejemplos de cómo la IA ha facilitado el desarrollo de nuevas formas de delitos cibernéticos más difíciles de detectar y contrarrestar. Esto ha incrementado la escala y efectividad de los ataques, redefiniendo el panorama del cibercrimen.

Se ha comprobado como el impacto del cibercrimen potenciado por la IA es profundo y multifacético y afecta tanto al ámbito económico como al social. En términos económicos, las empresas se enfrentan a costos crecientes en ciberseguridad y a la posibilidad de sufrir grandes pérdidas financieras debido a robos de datos y otros fraudes. Además, la pérdida de la confianza del cliente en las instituciones que no logran proteger adecuadamente sus datos acarrea consecuencias muy graves que pueden perpetuarse a lo largo del tiempo. Estos ataques también comprometen la estabilidad de los mercados financieros y lo hacen generando fluctuaciones e inestabilidad en la economía global. Desde una perspectiva social, la creciente sofisticación de los ataques ha generado una falta de confianza en las plataformas digitales y los usuarios se ven cada vez más vulnerables ante amenazas como el robo de identidad y la manipulación de información, lo que afecta su percepción sobre la seguridad en línea.

Para enfrentar esta situación, es imperante desarrollar marcos normativos que regulen el uso de la IA en el cibercrimen. Estos marcos deben tener en cuenta tanto aspectos legales como éticos. La regulación debe ser lo suficientemente flexible para adaptarse a las rápidas evoluciones tecnológicas y, a la vez, lo suficientemente rigurosa para garantizar que los desarrolladores y los operadores de sistemas de IA no lleven a cabo desigualdades o vulneren derechos fundamentales. Un marco ético sólido no sólo es necesario para regular el uso de la IA, sino también para garantizar que estas tecnologías no sean utilizadas con fines maliciosos.

Un desafío clave en esta nueva era es la responsabilidad jurídica. La capacidad de la IA para actuar de manera autónoma plantea preguntas sobre quién debe ser considerado responsable cuando una IA comete un delito. Actualmente, el derecho penal tradicional asigna responsabilidad a personas físicas o jurídicas, pero, con la IA surgen nuevos desafíos ya que muchas veces estas tecnologías pueden actuar sin intervención humana directa. Por tanto, ha quedado claro que esto requiere una revisión de los conceptos tradicionales de responsabilidad y la creación de nuevos marcos legales que aborden estos dilemas.

Ante la complejidad de los ciberataques actuales, también es inexcusable implementar estrategias tecnológicas avanzadas. Tecnologías como el *blockchain* y el *machine learning* han demostrado ser herramientas útiles para la detección temprana de amenazas y la protección de datos. Las empresas y los gobiernos deben invertir en estas tecnologías para reforzar sus defensas digitales. Sin embargo, como hemos visto, ninguna estrategia tecnológica será completamente efectiva sin una cooperación internacional sólida. El

cibercrimen no conoce fronteras, por lo que es fundamental que los países armonicen sus normativas y colaboren en la persecución de estos delitos. Sólo a través de una cooperación global será posible mitigar el impacto del cibercrimen en una economía cada vez más digitalizada.

No se debe subestimar la importancia de la educación y concienciación en la lucha contra el cibercrimen. Muchos ataques cibernéticos como el *phishing* y el *ransomware*, explotan la falta de conocimiento de los usuarios sobre las mejores prácticas de seguridad digital. La creación de una cultura de ciberseguridad, tanto a nivel individual como organizacional, es esencial para mitigar los riesgos. Las organizaciones deben invertir en la formación continua de sus empleados, especialmente en sectores tan críticos como son el financiero y el sanitario. Además, la concienciación pública y las campañas educativas pueden reducir significativamente el número de ataques al aumentar la capacidad de los usuarios para identificar y responder a las amenazas.

Para concluir, la irrupción de la inteligencia artificial en el ámbito del cibercrimen ha transformado el panorama de la seguridad digital. Ha presentado desafíos sin precedentes para las empresas, los gobiernos y la sociedad en general. Únicamente mediante la combinación de estrategias tecnológicas avanzadas, una regulación adecuada, la cooperación internacional y la concienciación de los ciudadanos, será posible enfrentar de manera efectiva las amenazas que plantea el cibercrimen en esta era de la IA. En este caso, la IA, al igual que otras tecnologías disruptivas, presenta un potencial tanto para el bien como para el mal; en consecuencia, efectivamente, la clave para aprovechar sus beneficios mientras se mitigan sus riesgos radica en la forma en la que gestionamos su desarrollo y aplicación.

REFERENCIAS DE FUENTES CITADAS

ÁVILA NIÑO, Fredy Yesid; RINCÓN NÚÑEZ, Paola Maritza. Inclusión de la formación en prevención y atención de delitos informáticos en la educación policial. **Revista educación**, v. 42, n. 2, p. 1-28, 2023. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=9392396.

ARA PINILLA, Ignacio. El difuso fundamento normativo de los derechos humanos. **Revista ESMAT**, n. 26, p. 285-302, 2023.

AYERBE, Ana. La ciberseguridad y su relación con la inteligencia artificial. **Análisis del Real Instituto Elcano (ARI)**, n. 128, p. 1-8, 2020. Disponible en: https://media.realinstitutoelcano.org/wp-content/uploads/2021/10/ari128-2020-ayerbe-ciberseguridad-y-su-relacion-con-inteligencia-artificial.pdf.

BECERRIL GIL, Anahiby Anyel. Retos para la regulación jurídica de la Inteligencia Artificial en el ámbito de la Ciberseguridad. **Revista IUS**, v. 15, n. 48, p. 9-24, 2021. Disponible en: https://www.scielo.org.mx/scielo.php?pid=S1870-21472021000200009&script=sci_arttext.

BONILLA BONILLA, Erika Viviana. **Propuesta de mejoramiento continuo de la seguridad informática y de la información en las instituciones de educación superior**. Bogotá D.C.: Universidad Santo Tomás, 2019. Disponible en: https://repository.usta.edu.co/bitstream/handle/11634/20824/2019erikabonilla.pdf?sequence=15.

CHÁVEZ-BRAVO, Juan; MALPARTIDA-MÁRQUEZ, Darwin; VILLACORTA-CAVERO, Armando; ORELLANO-ANTÚNEZ, Juan. La influencia de la automatización inteligente en la detección del cibercrimen financiero. **Boletín de Coyuntura**, n. 31, p. 26-33, 2021. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8488976.

DE LA CUESTA AGUADO, Paz M. Inteligencia artificial y responsabilidad penal. **Revista penal México**, n. 16 y 17, p. 51-62, 2020. Disponible em: https://dialnet.unirioja.es/servlet/articulo?codigo=7675764.

DOLADER RETAMAL, Carlos; BEL ROIG, Joan; MUÑOZ TAPIA, José Luis. La blockchain: fundamentos, aplicaciones y relación con otras tecnologías disruptivas. **Economía industrial**, n. 405, p. 33-40, 2017. Disponible em: https://dialnet.unirioja.es/servlet/articulo?codigo=6207510.

ESTER SÁNCHEZ, Antonio Tirso. El desafío de la Inteligencia Artificial a la vigencia de los derechos fundamentales. **Cuadernos Electrónicos de Filosofía del Derecho**, n. 48, p. 111-139, 2023. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8962445.

ESTUARDO DUARTE, Carlos. Ciberdelincuencia: análisis del Convenio No. 85 de Budapest y el compromiso del Estado de Guatemala. **Revista Ciencia Multidisciplinaria CUNORI**, v. 5, n. 2, p. 111-118, 2021. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8873588.

FERNÁNDEZ MARTÍNEZ, Luis Felipe. Reflexiones sobre la ética y la era digital. **Cuadernos Fronterizos**, n. 61, p. 20-24, 2024. Disponible em: https://erevistas.uacj.mx/ojs/index.php/cuadfront/article/view/6532/8161.

FERNÁNDEZ RODRÍGUEZ, José Julio. Aproximación crítica a la manipulación informativa: el ejemplo de las redes sociales. **Gladius et Scientia. Revista de Seguridad del CESEG**, n. 3, p. 1-23, 2021. Disponible em: https://revistas.usc.gal/index.php/gladius/article/view/8909.

GARCÍA DEL POYO, Rafael. La seguridad jurídica en el entorno digital. **Revista de Estudios Jurídicos**, n. 13, p. 182-202, 2013. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=5255445.

GONZÁLEZ ARENCIBIA, Mario; MARTÍNEZ CARDERO, Dagmaris. Dilemas éticos en el escenario de la inteligencia artificial. **Economía y sociedad**, v. 25, n. 57, p. 1-17, 2020.

Disponible en: https://www.scielo.sa.cr/scielo.php?pid=S2215-34032020000100093&script=sci_arttext.

GONZÁLEZ LÓPEZ, Édgar. Los derechos digitales fundamentales ¿es necesaria su reconfiguración en el ordenamiento jurídico? **Revista de Derecho Administrativo**, n. 20, p. 234-267, 2021. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8510534.

GUAÑA-MOYA, Javier. La importancia de la seguridad informática en la educación digital: retos y soluciones. **RECIMUNDO: Revista Científica Mundo de la Investigación y el Conocimiento**, v. 7, n. 1, p. 609-616, 2023. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8977055.

HERNÁNDEZ GIMÉNEZ, María. Inteligencia artificial y derecho penal. **Actualidad jurídica iberoamericana**, fasc. 2, n. 10, p. 792-843, 2019. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6978830.

INSTITUTO NACIONAL DE CIBERSEGURIDAD. **Pongamos en práctica la ciberhigiene**. Página web. Disponible en: https://www.incibe.es/ciudadania/blog/pongamos-en-practica-la-ciberhigiene.

JIMÉNEZ BERNALES, Luis Alberto. El estado actual del cibercrimen en Perú y el derecho alemán. **Boletín Mexicano de Derecho Comparado**, v. 56, n. 167, p. 197-219, 2023. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=9529435.

LEÓN CAMINO, Arantza. **El agente encubierto virtual**. Tesis doctoral, Universidad Carlos III de Madrid, 2022. Disponible en: https://e-archivo.uc3m.es/rest/api/core/bitstreams/9350c3b3-b6d1-4cd0-aaae-7fc89480472a/content.

LÓPEZ BARONI, Manuel Jesús. Las narrativas de la inteligencia artificial. **Revista de bioética y derecho**, n. 46, p. 5-28, 2019. Disponible en: https://scielo.isciii.es/scielo.php?pid=S1886-58872019000200002&script=sci_arttext.

MARTÍNEZ SANTANDER, Carlos José et al. Seguridad por capas para frenar ataques de Smishing. **Dominio de las Ciencias**, v. 4, n. 1, p. 115-130, 2018. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6255067.

MERINO AJILA, Francisco Javier. Evolución internacional de la legislación sobre ciberdelincuencia tras el Convenio de Budapest. **Ciencia Latina: Revista Multidisciplinar**, v. 8, n. 3, p. 3654-3671, 2024. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=9610593.

MILLER, Tim. Explanation in artificial intelligence: insights from the social sciences. **Artificial Intelligence**, v. 267, p. 1-38, 2019. Disponible en: https://www.sciencedirect.com/science/article/pii/S0004370218305988.

MIRANDA GONÇALVES, Rubén. Ethics, Technology and Rights: challenges to justiciability in the digital environment. **Legal and administrative studies**, v. 29, n. 2, p. 61-84, 2023. Disponible en: https://www.upit.ro/_document/304243/jlas_2_2023.pdf.

MIRANDA GONÇALVES, Rubén. Inteligencia artificial y derechos humanos: una solución a los conflictos éticos y morales a través de una regulación normativa futura. In: MIRAUT MARTÍN, Laura; ZALUCKI, Mariusz (Editores); MIRANDA GONÇALVES, Rubén; PARTYK, Aleksandra (Coordinadores). **Artificial Intelligence and Human Rights**. Madrid: Dykinson, 2021, p. 48-76.

MIRANDA GONÇALVES, Rubén; MOREIRA DOMINGOS, Isabela. Gobernanza blockchain: tecnología disruptiva para el control de la corrupción en la salud pública. **Revista Jurídica UNICURITIBA**, v. 4, n. 66, p. 31-49, 2021. Disponible en: http://hdl.handle.net/10553/113785.

MIRAUT MARTÍN, Laura. **La formulación jurídica del libre desarrollo de la personalidad**. Madrid: Dykinson, 2023.

MIRAUT MARTÍN, Laura. **La implicación del concepto de probabilidad en el derecho**. Murcia: Laborum Ediciones, 2023.

MIRAUT MARTÍN, Laura. El sentido de las generaciones de derechos humanos. **Cadernos de Dereito Actual**, n. 19, p. 431-446, 2022. Disponible en: https://www.cadernosdedereitoactual.es/ojs/index.php/cadernos/article/view/894.

MIRÓ LLINARES, Fernando. La respuesta penal al ciberfraude. Especial atención a la responsabilidad de los muleros del phishing. **Revista Electrónica de Ciencia Penal y Criminología**, n. 15, p. 1-56, 2013. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4407809.

MONASTERIO ASTOBIZA, Aníbal. Ética para máquinas: similitudes y diferencias entre la moral artificial y la moral humana. **Dilemata. Revista Internacional de Éticas Aplicadas**, n. 30, p. 129-147, 2019. Disponible en: https://dilemata.net/revista/index.php/dilemata/article/view/412000295.

MORÁN ESPINOSA, Alejandra. Responsabilidad penal de la Inteligencia Artificial (IA). ¿La próxima frontera? **Revista IUS**, v. 15, n. 48, p. 289-323, 2021. Disponible en: https://www.scielo.org.mx/scielo.php?pid=S1870-21472021000200289&script=sci_arttext.

STUART, Russell; NORVIG, Peter. **Artificial Intelligence. A modern approach**. 2. ed. New Jersey: Prentice Hall, 2003.

PABLO-MARTÍ, Federico. **La Inteligencia Artificial General y sus riesgos**. Perspectivas SCCS: Explorando el Futuro de la Economía, Educación y Sociedad, p. 1-5, s.f. Disponible en: http://sccs.web.uah.es/wp/wp-content/uploads/2024/05/P2401-La-AGI-y-sus-riesgos.pdf.

PAYÁ SANTOS, Claudio; CREMADES GUISADO, Álvaro; DELGADO MORÁN, Juan José. El fenómeno de la ciberdelincuencia en España: la propuesta de la Universidad Nebrija en la

capacitación de personal para la prevención y el tratamiento del ciberdelito. **Revista Policía y Seguridad Pública**, v. 1, año 7, p. 237-270, 2017. Disponible en: https://camjol.info/index.php/RPSP/article/view/4312.

PECES-BARBA MARTÍNEZ, Gregorio. Sobre el fundamento de los derechos humanos un problema de Moral y Derecho. **Anales de la Cátedra Francisco Suárez**, n. 28, p. 193-208, 1988. Disponible en: https://revistaseug.ugr.es/index.php/acfs/article/view/12259/10152.

PÉREZ LUÑO, Antonio-Enrique. **Manual de Informática y derecho**. Barcelona: Ariel, 1996.

RAYÓN BALLESTEROS, María Concepción; GÓMEZ HERNÁNDEZ, José Antonio. Cibercrimen: particularidades en su investigación y enjuiciamiento. **Anuario Jurídico y Económico Escurialense**, n. 47, p. 209-234, 2014. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=4639646.

SÁNCHEZ VERA, Fulgencio; MARTÍNEZ GUIRAO, Javier Eloy; TÉLLEZ INFANTES, Anastasia. La seguridad en el ciberespacio desde una perspectiva sociocultural. **Methaodos. Revista de ciencias sociales**, v. 10, n. 2, p. 243-258, 2022. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8634381.

SUÁREZ-MIRA RODRÍGUEZ, Carlos. Internet y Derecho penal: viejos y nuevos delitos. In: FERNÁNDEZ RODRÍGUEZ, José Julio; SANSÓ-RUBERT PASCUAL, Daniel (Directores). **Internet: um nuevo horizonte para la seguridade y la defensa**. Santiago de Compostela: Universidad de Santiago de Compostela, 2010, p. 103-124.

TAPIA HERMIDA, Alberto Javier. La responsabilidad civil derivada del uso de la inteligencia artificial y su aseguramiento. **Revista Ibero-Latinoamericana de Seguros**, v. 30, n. 54, p. 107-146, 2020. Disponible en: https://revistas.javeriana.edu.co/index.php/iberoseguros/article/view/33793.

TAPIA SÁNCHEZ, Leónidas Salvador. Tecnología y derecho: una mirada al comercio electrónico, el cibercrimen y el soft law. **Ars Iuris Salmanticensis: AIS: revista europea e iberoamericana de pensamiento y análisis de derecho, ciencia política y criminología**, v. 10, n. 1, p. 199-226, 2022. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=8484220.

TEMPERINI, Marcelo GI; MACEDO, Maximiliano. La problemática de los perfiles falsos en Facebook y su relación con el Cibercrimen. **Simposio Argentino de Informática y Derecho (SID 2015) - JAIIO**, v. 4, p. 185-198, 2015. Disponible en: https://sedici.unlp.edu.ar/handle/10915/55608.

VERDUGO GUZMÁN, Silva. **Ciberespacio, Metaverso y nuevos delitos que gravitan sobre los derechos humanos**. Valencia: Tirant lo Blanch, 2023.

INFORMAÇÕES DO AUTOR

Rubén Miranda Gonçalves
Doctor en Derecho con mención internacional, Máster en Derecho de las Administraciones e Instituciones Públicas y Licenciado en Derecho, por la Universidad de Santiago de Compostela, España. Es profesor del área de Filosofía del Derecho en la Universidad de Las Palmas de Gran Canaria. Profesor tutor venia docendi en el Centro Asociado de Las Palmas de la Universidad Nacional de Educación a Distancia (UNED); Postdoctorado en Derecho por la Universidade do Estado do Rio de Janeiro. Email: ruben.miranda@ulpgc.es.

COMO CITAR

GONÇALVES, Rubén Miranda. Amenazas digitales: estrategias efectivas para enfrentar y combatir el cibercrimen. **Novos Estudos Jurídicos**, Itajaí (SC), v. 29, n. 3, p. 791-820, 2024. DOI: 10.14210/nej.v29n1.p791-820.

Recebido em: 13 de mai. de 2024
Aprovado em: 11 de nov. de 2024