Sinergia Académica ISSN: 2765-8252

Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024

Volumen: 7
Nro. 4
Año: 2024

Desafíos del derecho frente a los delitos de estafa coadyuvados por la inteligencia artificial (IA)

Challenges of the law against fraud crimes aided by artificial intelligence (IA)

Klever Patricio Galindo Espinosa[1] (kgalindoe@unemi.edu.ec) (https://orcid.org/0009-0004-6448-8911)

Mayerly Jamilex Briones Mendoza[2](mbrionesm4@unemi.edu.ec) (https://orcid.org/0009-0000-4747-8245)

Estefanny Sulay Suarez Jaramillo[3] (esuarezj@unemi.edu.ec) (https://orcid.org/0009-0008-5062-6526)

Galo Rafael Gallardo Lecaro[4] (ggallardol@unemi.edu.ec) (https://orcid.org/0009-0003-6581-9885)

Holguer Estuardo Romero Urréa[5] (hromerou@unemi.edu.ec) (https://orcid.org/0000-0002-0877-0339)

Resumen

La inteligencia artificial en la nueva era del Internet, ha tenido avances notables que nos ofrecen muchas herramientas innovadoras que son generadoras de manera sustancial en varios sectores estratégicos. Sin embargo, la delincuencia aprovecha esta tecnología para cometer delitos, la estafa, por ejemplo. Estos delitos han evolucionado a medida que los mismos delincuentes lo han hecho, ganando la competencia para poder dar uso a estas IA de la manera más idónea para el cometimiento de más actos delictivos. Este artículo tiene como fin el examinar tendencias asociadas de la IA con la estafa, así como los desafíos, problemas y obstáculos que enfrentarían los que investigan estos delitos.

[1] Estudiante de la Universidad Estatal de Milagro, Ecuador
[2] Estudiante de la Universidad Estatal de Milagro, Ecuador
[3] Estudiante de la Universidad Estatal de Milagro, Ecuador
[4] Estudiante de la Universidad Estatal de Milagro, Ecuador
[5] Docente de la Universidad Estatal de Milagro, Ecuador

Sinergia Académica
ISSN: 2765-8252
Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024
Volumen: 7
Nro. 4
Año: 2024

Entre los resultados se encuentran las dificultades que enfrentan los jueces para ajusticiar, la ausencia de legislación pertinente, la inexperiencia de los investigadores en la recopilación y análisis de pruebas digitales y la salvaguarda de la propia inteligencia artificial. Este artículo aborda los importantes desafíos que plantean los vacíos legales, las complejidades de la asignación de responsabilidades legales y la necesidad de revisar las regulaciones existentes a través del análisis exhaustivo. Para abordar estas cuestiones, se presentan recomendaciones, entre ellas el establecimiento de marcos jurídicos específicos para la IA, la mejora de las capacidades investigativas de entidades como la Fiscalía General del Estado y la Policía Nacional del Ecuador, la educación de los ciudadanos y los profesionales del derecho, así como el avance de las habilidades técnicas dentro del sector judicial para mitigar eficazmente los riesgos emergentes asociados a la IA.

Abstract

Artificial intelligence in the new era of the Internet has made remarkable progress, offering us many innovative tools that are substantially generating in several strategic sectors. However, criminals take advantage of this technology to commit crimes, such as fraud. These crimes have evolved as the criminals themselves have done, gaining the competition to be able to use this AI in the most suitable way to commit more criminal acts. This article aims to examine trends associated with AI and fraud, as well as the challenges, problems and obstacles that those investigating these crimes would face.

Among the results are the difficulties faced by judges in administering justice, the absence of relevant legislation, the inexperience of investigators in collecting and analyzing digital evidence, and the safeguarding of artificial intelligence itself. This article addresses the significant challenges posed by legal loopholes, the complexities of assigning legal responsibilities, and the need to review existing regulations through a comprehensive analysis. To address these issues, several recommendations are presented, including the establishment of specific legal frameworks for artificial intelligence, the improvement of the investigative capabilities of entities such as the Attorney General's Office and the National Police of Ecuador, the education of citizens and legal professionals, as well as

Klever Patricio Galindo Espinosa
Mayerly Jamilex Briones Mendoza
Estefanny Sulay Suarez Jaramillo
Galo Rafael Gallardo Lecaro
Holguer Estuardo Romero Urréa
Sinergia Académica
ISSN: 2765-8252
Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024
Volumen: 7
Nro. 4
Año: 2024

advancing technical skills within the judicial sector to effectively mitigate emerging risks associated with AI.

Palabras claves: inteligencia artificial, estafa, marcos jurídicos, responsabilidades legales, regulaciones

Keywords: artificial intelligence, fraud, legal frameworks, legal responsibilities, regulations

Introducción

En los últimos años, el desarrollo acelerado de la inteligencia artificial (IA) ha cambiado principalmente la forma en que interactuamos con el mundo digital y la forma en que se llevan a cabo ciertas actividades comerciales, financieras y sociales. Sin embargo, esta innovación tecnológica también trae consigo una serie de riesgos y desafíos legales sin precedentes, especialmente en el ámbito de los delitos de estafa. Al utilizar la inteligencia artificial para cometer estafa, los delincuentes se han vuelto más especialistas y pueden crear comportamientos engañosos altamente atractivo que son difíciles de detectar y castigar bajo el marco legal ecuatoriano. El objetivo de este estudio es analizar cómo se pueden utilizar las capacidades técnicas de la inteligencia artificial para facilitar los delitos de estafa y evaluar los desafíos que esto plantea al sistema jurídico, especialmente en términos de asignación de responsabilidad y adaptación de la normativa penal existente.

Entre 2022 y 2023 los casos de estafas mediante la utilización de sistemas de inteligencia artificial se han disparado mediante la utilización de imágenes, videos o audios manipulados, el último informe de la empresa inglesa Sumsub manifiesta que en Filipinas aumento 4.500% el intento de fraudes interanual, seguidos por otros países como EE. UU., Vietnam y Bélgica. En países de la región se ha visto un incremento de 411% en estafas con IA. En Ecuador se ha revelado una realidad alarmante sobre las denuncias de estafa según la Policía Nacional del Ecuador en entre los años 2022, 2023 y lo que va del 2024 se ha registrado 55830 denuncias por estafa (Policía Nacional del Ecuador, 2024) de las cuales persisten llamadas o mensajes de texto, manejo fraudulento y engaño, y los casos mediante

Sinergia Académica ISSN: 2765-8252
Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024
Volumen: 7
Nro. 4
Año: 2024

estafas con IA paso del 0,81% en 2021 al 1.06% en el 2023 (*Sumsub Identity Fraud Report*, 2023).

El objetivo central del estudio es identificar los principales métodos de estafa mediante la IA, analizar y evaluar los vacíos jurídicos que existen actualmente para abordar estos delitos y desarrollar recomendaciones que puedan ayudar a los investigadores policiales, fiscalía y al poder judicial a abordar de manera efectiva este fenómeno. El estudio se realizó porque la estafa mediante inteligencia artificial es cada vez más frecuente y los sistemas investigativos y judiciales no están completamente preparados para afrontar esta nueva realidad. Si bien algunas jurisdicciones han comenzado a considerar la incorporación de regulaciones relacionadas con la IA. En Ecuador nuestros legisladores siguen siendo incapaces de abordar la autonomía y la complejidad de estos delitos, lo que crea un vacío legal y un entorno propicio a la impunidad. El estudio surgió de la preocupación por el rápido crecimiento de estos delitos, que afectan no solo a individuos sino también a empresas y al propio país. La capacidad de la IA para generar fraude a escala y con un alto grado de personalización supera las técnicas regulatorias y sancionadoras tradicionales, por lo que es imperativo que la ley se adapte a los desafíos que plantea esta.

Para lograr los objetivos planteados, este artículo empleará una metodología mixta que incluirá la revisión de literatura existente sobre la IA y la estafa, así como el análisis de tendencias de fraude con inteligencia artificial. Además, se analizarán estadísticas y datos de organismos oficiales y organizaciones no gubernamentales para proporcionar un contexto empírico sobre la prevalencia y las respuestas institucionales a la estafa. Esta combinación de enfoques permitirá una comprensión integral y multifacética del papel del derecho frente a los delitos de estafa coadyuvados por la IA.

Materiales y métodos

Para la realización de este artículo científico se emplearon métodos cualitativos y cuantitativos que van a permitir el entendimiento total de las estafas mediante el uso de inteligencia artificial y los desafíos del derecho en estos casos por lo cual inicialmente se llevó a cabo una exhaustiva revisión literaria sobre el uso de IA en estafas donde se

Sinergia Académica ISSN: 2765-8252
Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024
Volumen: 7
Nro. 4
Año: 2024

tomaron en cuenta artículos científicos, libros, informes técnicos de organizaciones internacionales y no gubernamentales, así como análisis de legislación y casos judiciales relevantes. Para la selección de estos recursos se tomó en cuenta información relevante y actual, con énfasis en trabajos publicados en la última década asegurándonos que provengan de fuentes confiables y de alta calidad.

Además, se realizó un análisis de las tendencias de fraude utilizando IA recolectando datos de informes anuales de ciberseguridad, estudio de casos y bases de datos de incidentes proporcionadas por la Policía Nacional del Ecuador, así como informes de la empresa inglesa Sumsub. Este análisis cualitativo se centró en identificar patrones similares, estrategias de IA utilizadas en fraudes, perfiles de los autores y las víctimas, así como métodos de prevención y detección que se utilizan.

También se utilizó un enfoque cuantitativo de datos obtenidos de organismos oficiales y organizaciones no gubernamentales para ofrecer un contexto empírico sobre la prevalencia de estas estafas y las respuestas institucionales ante ellas. Las fuentes abarcan datos de instituciones como Agencia de Ciberseguridad de la Unión Europea, el Centro Nacional de Ciberseguridad del Reino Unido, así como informes de la empresa inglesa Sumsub y las denuncias de estafa de la Policía Nacional del Ecuador. Utilizando estas estadísticas junto con diferentes delitos y frecuencias, y mediante un análisis crítico, se buscará determinar relaciones importantes entre la implementación de IA en las estrategias de seguridad y la reducción de estafas. La combinación de estos métodos permitió una evaluación total de la situación actual de las estafas en Ecuador mediante el uso de la IA, y el desafío del derecho penal y de las instituciones encargadas de investigar o juzgar este delito (Centro Nacional de Ciberseguridad del Reino Unido, 2023)

Resultados

Definiciones

La estafa según el Código Orgánico Integral Penal (COIP), en su artículo 186 establece lo siguiente.

Klever Patricio Galindo Espinosa
Mayerly Jamilex Briones Mendoza
Estefanny Sulay Suarez Jaramillo
Galo Rafael Gallardo Lecaro
Holguer Estuardo Romero Urréa
Sinergia Académica
ISSN: 2765-8252
Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024
Volumen: 7
Nro. 4
Año: 2024

> La persona que, para obtener un beneficio patrimonial para sí misma o para una tercera persona, mediante la simulación de hechos falsos o la deformación u ocultamiento de hechos verdaderos, induzca a error a otra, con el fin de que realice un acto que perjudique su patrimonio o el de una tercera, será sancionada con pena privativa de libertad de cinco a siete años (Código Orgánico Integral Penal (COIP), 2014).

La inteligencia artificial o más conocida como IA es "la tecnología que permite que las computadoras simulen la inteligencia humana y las capacidades humanas de resolución de problemas" (IBM, s.f.).

Tipos de estafas mediante la IA

Uso de Deepfake

"El llamado deepfake consiste en imágenes o videos que se generan por medio de una técnica de inteligencia artificial. Se trata de un aprendizaje automático llamado en inglés *deep learning* (en español: aprendizaje profundo)" (National Geographic, 2023) El uso de deepfake ha permitido a la delincuencia crear audios, fotos y videos más fácil y barato para engañar a personas y a los encargados de investigar estafas, las voces creadas con IA pueden ser usadas para realizar secuestros virtuales o intentar obtener información

Uso de Phishing avanzado con IA

El uso de los ataques Phishing es mediante el engaño a la víctima esta pueda revelar información confidencial, como información personal, contraseñas o números de tarjetas de crédito, haciendo pasar por alguien que no son. "La IA ha facilitado la labor de los cibercriminales a la hora de llevar a cabo sus ataques de phishing, escribiendo mensajes de phishing mucho más creíbles, imitando las voces de personas, investigando a los objetivos y generando Deepfakes" (D´Andrea, 2024).

Ingeniería social automatizada con el uso de la IA

La ingeniería social con el uso de la IA consiste en engañar a las víctimas para que les proporcionen información confidencial, la IA con la utilización de Chatbots son capaces de

Klever Patricio Galindo Espinosa
Mayerly Jamilex Briones Mendoza
Estefanny Sulay Suarez Jaramillo
Galo Rafael Gallardo Lecaro
Holguer Estuardo Romero Urréa
Sinergia Académica
ISSN: 2765-8252
Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024
Volumen: 7
Nro. 4
Año: 2024

entablar conversaciones con muchas personas o víctimas al mismo tiempo, simulando ser una persona real. La IA es capaz de interactuar con las víctimas para ganarse su confianza, sosteniendo conversaciones convincentes mediante chats, correos electrónicos y redes sociales, para poder obtener información.

Suplantación de identidad por voz con el uso de la IA

La clonación de voz es otro uso de la IA que ha facilitado fraudes complejos. A través de esta técnica, los delincuentes pueden utilizar la voz de un alto ejecutivo para que parezca que está hablando con un empleado o socio con la finalidad de ordenar pagos o entrega de información sensible. También la suplantación de voz de personas cercanas a la víctima puede ser amigo o familiares para solicitar dinero bajo pretextos falsos.

Planteamiento de las hipótesis

La falta de un Código Orgánico Integral Penal actualizado y especializado limita la capacidad de la parte investigativa policial y del sistema judicial ecuatoriano para abordar eficazmente los delitos de estafa facilitados por inteligencia artificial, ya que COIP en su artículo 186 no menciona el tema de estafas mediante la utilización de inteligencia artificial y el notable incremento en los últimos años, ha impulsado grandes ganancias económicas, para las personas que se dedican a este delito. Por tal motivo los operadores judiciales (jueces, fiscales, abogados) carecen de la formación necesaria para identificar y procesar este delito.

La concientización y la mejora de educación de los ciudadanos y de los profesionales del derecho en torno a este tema principal tratado reducirán de manera abismal la vulnerabilidad que se tiene frente a este tipo nuevo de delitos. Este fenómeno ha puesto en evidencia la falta de conocimiento en avances tecnológicos de todos nosotros, evidenciando la necesidad de encontrar una estrategia para combatir estos tipos de delitos, empezando desde nuestro conocimiento.

Discusión

Complejidad técnica en la tipificación penal

Klever Patricio Galindo Espinosa
Mayerly Jamilex Briones Mendoza
Estefanny Sulay Suarez Jaramillo
Galo Rafael Gallardo Lecaro
Holguer Estuardo Romero Urréa
Sinergia Académica
ISSN: 2765-8252
Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024
Volumen: 7
Nro. 4
Año: 2024

El desafío mayor en este tipo de delitos es la confusa naturaleza de los delitos perpetrados con el uso de inteligencia artificial. Tecnologías como los de sistemas de clonación y de los *deepfakes* producen un tipo de evidencia alterada de manera muy notable, lo que conllevaría a una complicación al momento de la diferenciación entre genuino y manipulado. Todos los profesionales del derecho, desde el abogado en libre ejercicio hasta el juez de mayor alto rango carecen de la experiencia necesaria para una interpretación correcta de la evidencia digital, complicando la catalogación del delito y de la manera de como pueda ser catalogado. Es por tal que la autonomía que ha ganado la IA, de manera conjunta con la dificultad de ser trazado, genera tergiversación al momento de determinar responsabilidad penal. ¿A quién se le atribuye el daño provocado? ¿Al que lo desarrolla, al que lo usa o a su propio algoritmo nato? Esta investigación pone de relieve las ambigüedades legales existentes en la regulación de las acciones realizadas o facilitadas por las tecnologías de IA.

Vacíos legales en la normativa ecuatoriana

En Ecuador, al igual que en muchos otros países, la estructura legal existente no está adecuadamente equipada para enfrentar los desafíos que presentan los delitos que involucran inteligencia artificial. La legislación actual está diseñada para abordar las formas tradicionales de fraude, incluidos el engaño y la falsificación, pero no tiene en cuenta los métodos emergentes en los que la tecnología facilita la manipulación avanzada y automatizada de la evidencia. Por ejemplo, la legislación en Ecuador carece de regulaciones explícitas relacionadas con los *deepfakes* y la clonación de voz, tecnologías que a menudo se emplean en la perpetración de estafas comerciales, robo de identidad o fraude financiero. El Código Orgánico Integral Penal no contiene cláusulas específicas que aborden los delitos cibernéticos avanzados que utilizan inteligencia artificial, lo que resalta la necesidad apremiante de actualizaciones legislativas que aborden adecuadamente los requisitos de este panorama digital en evolución.

Desafíos en la investigación forense digital

Klever Patricio Galindo Espinosa
Mayerly Jamilex Briones Mendoza
Estefanny Sulay Suarez Jaramillo
Galo Rafael Gallardo Lecaro
Holguer Estuardo Romero Urréa
Sinergia Académica ISSN: 2765-8252
Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024
Volumen: 7
Nro. 4
Año: 2024

El poder investigativo de estos delitos cibernéticos, incluyendo a las estafas facilitadas por la IA, depende de gran medida de la existencia de una ciencia forense digital y de una informática forense. Sin embargo, las complejidades son mayores porque los algoritmos que tienen las IA han ganado la capacidad de aprender de errores y de adaptarse para hacerlo mejor, lo que significa que las actividades ilícitas cometidas por esta son cada vez más sofisticadas y precisas, vulnerando así las defensas ya puestas y que antes les había ganado la partida. La capacidad de identificar y corroborar la manipulación de evidencia digital es muy limitada en muchos países, entre ellos Ecuador, es así que los organismos responsables de investigar estos delitos y de aplicar justicia en muchas de las ocasiones carecen de todo tipo de recurso para que detectar el delito sea posible, al igual con el reunir una evidencia digital creíble, lo que daría como resultado en un déficit en la capacidad del estado para batallar a estas formas de fraude en crecimiento.

Propuesta

La táctica general implicaría en el establecimiento de un marco del tipo regulatorio de amplio espectro que tenga un diseño fijo para enfrentar todo tipo de delito que esté relacionado con estafa por inteligencia artificial, esto sobre una base que tendría tres pilares primordiales: una actualización en materia legal y regulatoria que tengan relación con delitos que involucran IA; un mejoramiento en las capacidades en el campo de la informática forense; y de brindar una capacitación especializada con una colaboración de escala internacional estableciendo regulaciones tecnológicas unificadas.

La modificación del Código Orgánico Integral Penal para incorporar categorizaciones explícitas de delitos facilitados por inteligencia artificial: la legislación ecuatoriana debe describir explícitamente los tipos de estafas que utilizan inteligencia artificial, incluidos los *deepfakes*, la clonación de voz y varias otras manipulaciones digitales sofisticadas. Es fundamental implementar sanciones diferenciadas para la estafa tecnológica, incorporando factores agravantes que consideran la aplicación de tecnología avanzada, las repercusiones económicas y los desafíos asociados con la detección. Establecimiento de un marco regulatorio para las plataformas tecnológicas que facilitan el desarrollo o utilización de inteligencia artificial.

Klever Patricio Galindo Espinosa
Mayerly Jamilex Briones Mendoza
Estefanny Sulay Suarez Jaramillo
Galo Rafael Gallardo Lecaro
Holguer Estuardo Romero Urréa
Sinergia Académica ISSN: 2765-8252
Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024
Volumen: 7
Nro. 4
Año: 2024

Regular el avance de las tecnologías de IA para evitar su aplicación en actividades fraudulentas, exigiendo que las organizaciones adopten estrategias preventivas e implementen sistemas de alerta temprana. Crear un marco de responsabilidad compartida para los proveedores de servicios de IA cuando sus tecnologías se empleen con fines ilícitos

Mejorar las competencias forenses y de investigación digital: establecer una unidad dedicada a abordar los delitos asistidos por IA dentro de la Policía Nacional del Ecuador. Brindar capacitación a jueces, fiscales y especialistas en análisis forense de IA, centrándose en metodologías para identificar *deepfakes*, clonación de voz y diversas formas de manipulación digital. Asignar recursos a tecnologías sofisticadas de detección forense destinadas a analizar evidencia digital alterada por inteligencia artificial, incluido software para la detección de deepfakes y el reconocimiento de patrones indicativos de fraude digital. Facilitar la cooperación internacional y establecer acuerdos bilaterales.

Colaboración internacional y convenios bilaterales: fomentar la colaboración global estableciendo acuerdos con naciones que enfrentan desafíos análogos, a la vez que se intercambia información y prácticas ejemplares en materia de regulación de los delitos cibernéticos y el uso indebido de la inteligencia artificial. La participación proactiva de Ecuador en organizaciones internacionales, incluidas Interpol y Europol, ha sido fundamental en la supervisión y gestión de los delitos cibernéticos transnacionales facilitadas por la IA (Europol, 2023).

Iniciativas de educación y concientización pública: establecer iniciativas educativas destinadas a aumentar la conciencia sobre los peligros de las estafas con IA entre el público en general, las empresas y los funcionarios gubernamentales, junto con estrategias para la prevención. Además, crear un sistema de alerta pública para notificar a los ciudadanos cuando se identifiquen estafas tecnológicas significativas que utilicen IA, ofreciéndoles orientación sobre cómo reconocer esas actividades fraudulentas.

Conclusión

El avance de la inteligencia artificial está transformando numerosos sectores, pero al mismo tiempo introduce desafíos significativos para el derecho penal al permitir tipos innovadores

Sinergia Académica ISSN: 2765-8252
Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024
Volumen: 7
Nro. 4
Año: 2024

de fraude que superan los métodos convencionales de regulación y supervisión. Este artículo ilustra que el sistema legal ecuatoriano enfrenta varios obstáculos clave para una respuesta efectiva, incluidas las deficiencias regulatorias, la preparación técnica insuficiente de los funcionarios de justicia y las complejidades de la investigación forense digital. Todas estas nuevas técnicas delictivas estudiadas en este trabajo han complicado con el identificar a los verdaderos infractores, sino que también complica el cómo la responsabilidad sería impuesta, esto debido a la autonomía que la IA ha ganado últimamente.

Es muy notable que el marco legal que actualmente tenemos dentro del Código Orgánico Integral Penal necesita una revisión para de esta manera poder incorporar estos tipos de delitos informáticos asistidos por la IA, para así asegurar que los que cometan estas infracciones tengan su merecida sanción. También, es necesario el integrar factores del tipo agravante en estas sanciones, sobre todo, cuando la IA sea empleada en estas infracciones que buscan el llevar ventajas económicas o el de manipular la información para un fin mucho más complejo. Sin tener este avance regulatorio, el impartir la justicia estará en desventaja en relación al aumento desmedido de estos delitos tecnológicos.

La capacidad limitada del tipo investigativo que el sistema judicial tiene, es un problema de lo más crítico, por lo que requiere que se cree unidades especializadas en delitos cibernéticos y también con capacitación continua de los profesionales del derecho y peritos que forman parte de este sistema. El poco o nulo conocimiento de informática forense complica a los operadores de la justicia, ya que no se podrá diferenciar la evidencia entre auténtica o aquella falsa que ha sido manipulada por el IA. La complejidad que este proceso crea, conlleva a la imprecisa clasificación de los delitos al igual que con la asignación de responsabilidades legales. Es muy importante que el Estado destine recursos para que estas tecnologías forenses avancen y sirvan para la formación técnica de personal, facilitando las investigaciones de estos tipos de delitos.

El tipo de naturaleza de estos delitos exige necesariamente una cooperación eficaz del tipo transfronteriza y de establecer normas comunes para facilitar la investigación y el procesamiento de los delincuentes, esto sin importar su ubicación geográfica. Con este contexto, es primordial de que nuestro país cree colaboraciones con organizaciones

Klever Patricio Galindo Espinosa
Mayerly Jamilex Briones Mendoza
Estefanny Sulay Suarez Jaramillo
Galo Rafael Gallardo Lecaro
Holguer Estuardo Romero Urréa
Sinergia Académica ISSN: 2765-8252
Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024
Volumen: 7
Nro. 4
Año: 2024

internacionales como la Interpol y Europol, y también el establecer acuerdos bilaterales que ayuden a promover el intercambio de información y mejores habilidades contra el fraude cibernético. En pocas palabras el poder pelear contra estos delitos implica en un esfuerzo colectivo del tipo mundial, caso contrario, el luchar contra estos delitos sería algo insuficiente en relación con el exponencial crecimiento de los delincuentes que explotan este tipo de delitos.

Es imperativo de que la ley avance de manera conjunta con los avances tecnológicos, adaptando estrategias dirigidas al futuro, no solo abordando actos delictivos mediante un castigo, sino que también tratar de evitarlos mediante ajustes del tipo regulatoria y mejorando las instituciones. Si bien es esencial de que los sectores judiciales y de aplicación de la ley deben de ser fortalecidos, también es importante tener una estrategia que permita anticipar a los avances de la inteligencia artificial. Así se podría crear un marco jurídico sólido, equipado para enfrentarse a los nuevos desafíos que presenta la IA, esto sin trasgredir a los principios fundamentales de la justicia ni de los derechos individuales.

Como resumen, para que podamos abordar de manera eficaz estas estafas asistidas por la IA es necesaria una estrategia integral que contemple el modernizar las leyes penales, las investigaciones forenses, colaboración internacional y el concienciar, de manera general, a la sociedad. Si estas sugerencias se logran ejecutar de manera coordinada, nuestro país al igual que varios otros, estarían mejor equipados para enfrentar a las estafas tecnológicas que aparezcan, y así garantizar una administración de justicia eficiente que cuida a la sociedad de todo tipo de riegos inherente que puedan estar asociados a este tipo de avances tecnológicos.

Referencias

D´Andrea, A. (2024, September 13). *Keeper.* https://www.keepersecurity.com/blog/es/2024/09/13/how-ai-is-making-phishing-attacks-more-dangerous/

Sinergia Académica ISSN: 2765-8252

Recepción: 08-07-2024 / Revisión: 13-09-2024 / Aprobación: 29-09-2024 / Publicación: 27-10-2024

Volumen: 7
Nro. 4
Año: 2024

Centro Nacional de Ciberseguridad del Reino Unido. (2023, agosto 3). *El NCSC y sus aliados revelan las vulnerabilidades cibernéticas más comunes explotadas en 2022*. Centro Nacional de Seguridad Cibernética.

Código Orgánico Integral Penal (COIP). (2014). *Delitos contra el derecho a la propiedad*. Lexis.

Europol. (2023). *Internet Organised Crime Threat Assessment*. Publications Office of the European Union, Luxembourg.

Policía Nacional del Ecuador. (2024). *Sistema David20i2*. Quito.

Sumsub Identity Fraud Report. (2023). chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://sumsub.com/files/sumsub_identity_fraud_report_2023.pdf?utm_campaign=fraud_report2023-link&utm_medium=automation&utm_source=email&vgo_ee=f72S0utw%2BlEnhcPtxwJRKyABYBKGnQk69p95Mcd%2ByL4LwKpT9%2BQ%3