Revista de Climatología

Volumen 23 Edición Especial Ciencias Sociales

Vol. 23 (2023): 4177-4187 ISSN 1578-8768

La zozobra social condicionada por la pandemia hacia una neo criminalidad

Lutgarda Palomino Gonzales[1]*, David Saúl Paulett Hauyon[1], Juan Manuel Ñiquen Quesquén[1], Manuel Moisés Valdivia Cotrina[1]

[1] Escuela de Posgrado. Universidad César Vallejo. Perú.

*Autor para correspondencia: Lutgarda Palomino Gonzales, luupago14@gmail.com

(Recibido: 10-12-2023. Publicado: 31-12-2023.)

DOI: 10.59427/rcli/2023/v23cs.4177-4187

Resumen

La conectividad a la red y la adopción de dispositivos digitales generó un ambiente propicio para el aumento de la comisión de delitos, tales como la extorsión, estafa, entre otros delitos que involucran el engaño a las personas a fin de obtener dinero o información personal. Por tanto, el objetivo general fue determinar de qué manera la zozobra social ha sido condicionada por la pandemia hacia una neo criminalidad. La metodología empleada fue tipo básica, diseño fenomenológico hermenéutico y enfoque cualitativo. Se concluyó que la inteligencia artificial en el ámbito del crimen influye a través de la suplantación de identidades, dado que la inteligencia artificial es empleada por los delincuentes para generar perfiles ficticios en línea y asumir identidades ajenas con propósitos fraudulentos.

Palabras claves: *Zozobra social, neo criminalidad, inteligencia artificial, crimen, delincuencia cibernética.*

Abstract

Network connectivity and adoption of digital devices generated an environment conducive to the increase in commission of crimes, such as extortion, fraud, among other crimes involve deceiving people in order to obtain money or personal information. Therefore, the general objective was to determine how social anxiety has been conditioned by pandemic towards neocriminality. The methodology used was basic type, hermeneutic phenomenological design and qualitative approach. It was concluded thatartificial intelligence in the field of crime influences through identity theft, given that artificial intelligence is used by criminals to generate fictitious online profiles and assume identities of others for fraudulent purposes.

Keywords: *Social anxiety, neocriminality, artificial intelligence, crime, cybercrime.*

1. Introducción

La investigación acerca de cómo los delincuentes eligen sus ubicaciones para cometer crímenes, ha resultado de gran importancia para entender los patrones de movilidad de los criminales y para analizar los motivos que influyen en la distancia que recorren para cometer actos delictivos. Por ejemplo, el hecho de que la mayoría de los delitos ocurran en las cercanías de la residencia de los delincuentes o de lugares donde realizan sus actividades diarias refleja una tendencia, y la probabilidad de que ocurra un delito, pero a medida que nos alejamos de esos puntos de referencia, no obstante, en el contexto de esta regla general, existen ciertos lugares que ofrecen oportunidades particularmente atractivas para la comisión de delitos o comportamientos antisociales (Trinidad et al., 2021). El ciberdelito, más que cualquier otra categoría de delito, trasciende fronteras y naciones, con los perpetradores, las víctimas y las evidencias a menudo dispersas por todo el mundo. El enjuiciamiento efectivo de los delitos cibernéticos se ve obstaculizado por la falta de armonización internacional y la diversidad de leyes nacionales en lo que respecta a la tipificación de delitos cibernéticos, la jurisdicción y los mecanismos de cooperación, todo ello exacerbado por las diferencias legales y constitucionales, que incluyen distintas interpretaciones de los derechos y la privacidad. Los Estados han adoptado y trasladado sus funciones estatales tradicionales al ámbito transnacional, lo que ha llevado a la creación de estados fragmentados, perpetuando así las deficiencias en la gestión de los delitos cibernéticos (Stambøl y Solhjell, 2021).

Es por ese motivo los países han estado desarrollando y poniendo en práctica sistemas basados en inteligencia artificial para combatir la delincuencia y la corrupción, con la esperanza de que estas herramientas tengan un impacto positivo. No obstante, todavía se carece de evidencia empírica sólida sobre la eficacia de estos sistemas automatizados diseñados para detectar y prevenirlos. La tecnología basada en inteligencia artificial ha sido adaptada por expertos en tecnología en el sector público, que trabajan en agencias encargadas de hacer cumplir la ley, así como por ciudadanos con habilidades técnicas, quienes se dedican a tareas como la recopilación y verificación de grandes conjuntos de datos. El objetivo es supervisar, identificar, informar y predecir riesgos, así como señalar posibles actividades ilícitas. (Odilla, 2023) De manera intrigante, los niveles de fraude no siguen la misma tendencia que otros delitos. Diversos estudios sugieren que, en general, las tasas de criminalidad están disminuyendo en el mundo occidental. Sin embargo, de manera contrastante, en los últimos años, las estadísticas de fraude muestran aumentos preocupantes. Este fenómeno es especialmente notable en los Estados Unidos, el Reino Unido y los Países Bajos. Por ejemplo, en los Países Bajos, entre 2005 y 2017, los casos de engaño se incrementaron en un factor de 2.3, los de falsificación en un factor de 2.4, los de extorsión en un factor de 1.8 y los de piratería informática en un factor de 3.9. (Junger et al, 2020).

Sin embargo, numerosos estudios han confirmado que los primeros confinamientos impuestos en respuesta a la pandemia de COVID-19 provocaron cambios en las actividades diarias de las personas y, por ende, en las tasas de delincuencia. Mientras que varios tipos de delitos violentos y contra la propiedad experimentaron disminuciones inmediatas después del primer confinamiento, los delitos en línea mostraron un aumento. Sin embargo, se ha investigado poco la relación entre los confinamientos sucesivos y cómo afectan a la delincuencia a medio plazo. Además, pocos estudios han examinado las posibles diferencias en las tendencias de delitos en línea y fuera de línea utilizando el mismo conjunto de datos. (Buil-Gil et al, 2021). En esa idea, se ha considerado pertinente como objetivo general de la presente investigación determinar de qué manera la zozobra social ha sido condicionada por la pandemia hacia una neo criminalidad. Del mismo modo se han considerado como objetivos específicos, analizar cómo facilita el empleo de herramientas tecnológicas en estafas y extorciones generando zozobra en la sociedad e identificar cómo afecta el robo de identidad para cometer fraudes financieros en nombre de la víctima.

2. Bases teóricas de la investigación

En las últimas dos décadas, ha habido un notable aumento en el estudio de cómo se distribuye la delincuencia en el espacio, y el análisis a pequeña escala o a nivel micro ha tomado la delantera en la investigación centrada en la ubicación. Esta tendencia ha sido impulsada por la mayor disponibilidad de datos sobre delitos que están geográficamente referenciados y por los avances tecnológicos en software que facilitan el análisis de cómo los delitos se agrupan en el espacio, conocido como análisis de puntos críticos. Sin embargo, este crecimiento en el análisis espacial quizás no haya sido igualado por avances similares en el análisis temporal de la delincuencia. (Newton y Felson, 2015).

Sin embargo, los rápidos cambios en los niveles de delincuencia durante la pandemia de COVID-19 y su posible relación con las explicaciones a largo plazo para la disminución de la delincuencia a nivel internacional pueden estar vinculados al aumento de la delincuencia cibernética, el fraude y otros delitos emergentes, debido a las nuevas oportunidades delictivas que se han presentado. Además, se sugiere que las políticas y prácticas centradas en la reducción de oportunidades delictivas pueden tener un impacto desproporcionado en la delincuencia juvenil. En otras palabras, la estrategia de reducir las oportunidades delictivas puede ser eficaz para abordar la delincuencia, especialmente entre los jóvenes, y que esta estrategia podría tener un impacto positivo a largo plazo en la reducción de la delincuencia. (Halford, 2020).

Se puede presumir que la inteligencia artificial puede servir como una herramienta en la comisión de delitos. Esto incluye el uso de la IA para predecir el comportamiento de personas o instituciones y aprovechar su vulnerabilidad, generar contenido falso para chantajear o dañar la reputación, y llevar a cabo acciones que los criminales humanos no pueden o no desean realizar debido a limitaciones físicas o de otro tipo. No obstante, la propia IA puede ser el blanco de actividades delictivas. Esto involucra eludir sistemas de seguridad que protegen contra delitos, evadir la detección o el castigo por delitos ya cometidos, y causar fallos o comportamientos erráticos en sistemas críticos o confiables, con el objetivo de causar daños o socavar la confianza pública. (Caldwell, 2020).

La perspectiva de elección racional es un marco teórico que se utiliza para entender eventos delictivos y orientar estrategias de prevención situacional. Esta perspectiva explica cómo las personas eligen de manera consciente y deliberada cometer actos criminales. Los individuos que consideran cometer delitos toman decisiones que buscan maximizar sus beneficios personales y minimizar los costos personales, como el riesgo de ser arrestados. Es importante destacar que estas decisiones no necesariamente son completamente racionales ni se planifican cuidadosamente debido a las limitaciones y circunstancias en las que se toman, lo que significa que los delincuentes operan con una forma de racionalidad limitada. (O'Hara et al, 2020).

Sin embargo, es comprensible que la revolución de las tecnologías de la información y la aparición del ciberespacio hayan tenido un impacto en los delitos físicos. En lo que respecta a la disminución de la delincuencia, es importante destacar que el cibercrimen no fue la causa principal de la disminución de la delincuencia en general. La disminución de la delincuencia no se debió a un factor específico, pero la llegada del ciberespacio como un nuevo ámbito de oportunidades criminales y el aumento de la ciberdelincuencia afectaron de manera significativa a ciertas formas específicas de delincuencia que estaban disminuyendo. (Miró-Llinares y Moneva, 2019).

Las personas a veces pasan por alto los riesgos de revelar inadvertidamente información personal, lo que podría aumentar su susceptibilidad a la victimización. Esto se debe a un deseo de socializar y destacar sus logros, a menudo superando su precaución natural. La información espacial y temporal única disponible en las redes de seguimiento de actividades en línea podría permitir a los delincuentes predecir con alta probabilidad dónde vive una posible víctima y sus patrones de actividad. En base a estos hallazgos, se puede concluir que las redes de seguimiento en línea tienen el potencial de ser utilizadas en varios tipos de delitos, tanto en entornos domésticos como en lugares públicos. En resumen, esta investigación destaca la posibilidad de que la delincuencia tradicional se vuelva cada vez más digitalizada. (Stottelaar, 2014).

Debido a la amplia conectividad a Internet y el uso generalizado de dispositivos digitales que han creado un entorno propicio para la proliferación de estafas que involucran intentos de engañar a las personas para que entreguen dinero o información personal. Se ha comprobado que estos esquemas tienen un impacto significativo en las víctimas, causando daños de naturaleza social, psicológica, emocional y económica. Por lo tanto, existe una sólida justificación para mejorar nuestra comprensión de las estafas y encontrar formas de prevenirlas. Una de las formas de abordar este problema es mediante la creación de guiones de delitos, un enfoque analítico que busca describir los procesos subyacentes que respaldan la comisión de estos delitos. (Lwin y Birks, 2023).

El mecanismo principal que se ha propuesto para explicar cómo el cibercrimen podría haber contribuido a la disminución de la delincuencia es el concepto de "desplazamiento atractivo". Según esta idea, los delincuentes podrían estar reemplazando la comisión de delitos físicos por delitos en línea que consideran más atractivos. Sin embargo, en general, es difícil identificar cómo los delitos cibernéticos podrían ser sustitutos efectivos de los delitos físicos. El cibercrimen requiere conjuntos de habilidades, experiencia, herramientas y recompensas bastante diferentes en comparación con los delitos físicos tradicionales. (Farrell y Birks (2018).

La realidad virtual no solo amplía las posibilidades de mejorar los métodos de recopilación de datos existentes, como las viñetas empleadas por los investigadores en los campos de la disuasión y la toma de decisiones penales, sino que también ofrece oportunidades para estudiar fenómenos que son prácticamente imposibles de abordar por razones prácticas, financieras o éticas mediante otros medios, como los robos en tiempo real o situaciones de gran aglomeración. Además, la tecnología de realidad virtual puede superar el desafío metodológico de equilibrar el control experimental y el realismo cotidiano, ya que combina altos niveles de realismo con un riguroso control experimental. (Van- Gelder et al, 2014).

Reconocer que el delito cibernético es amplio y a menudo carece de precisión. Por lo general, se pueden distinguir tres categorías generales de delitos cibernéticos. En primer lugar, los delitos contra las computadoras implican el acceso no autorizado a sistemas informáticos, como intrusiones cibernéticas o hacking, donde las computadoras son el objetivo del ataque. En segundo lugar, los delitos que utilizan computadoras, comúnmente conocidos como "delitos cibernéticos", son aquellos en los que se utilizan tecnologías de la información y la comunicación para cometer un delito, como el robo de identidad, el phishing y el uso fraudulento de tarjetas de crédito en línea. En tercer lugar, los delitos .^{en}çomputadoras se refieren a aquellos en los que el contenido en sí mismo constituye el delito. (Reep-van, 2018).

El sistema de justicia penal se asemeja comúnmente a un embudo, ya que recibe numerosos informes de delitos, pero solo una pequeña proporción resulta en la condena de delincuentes. Pocos informes de delitos se convierten

en investigaciones policiales, y aún menos investigaciones culminan en casos judiciales. Aunque las sentencias judiciales proporcionan información sobre las condenas, gran parte del proceso queda sin visibilidad. Hoy en día, tanto las empresas tecnológicas como los gobiernos tienen un mayor acceso a la información, gracias a la vigilancia tanto en línea como fuera de línea. El cifrado es una de las pocas tecnologías disponibles que permite a ciudadanos, empresas y otras a proteger la privacidad de manera legal. Sin embargo, los delincuentes también hacen uso de esta tecnología. (Hartel y Van, 2023).

Las habilidades en tecnologías de la información y comunicación son un factor importante en dos de cada tres preocupaciones clave en el estudio de casos relacionados con delitos en línea. Pues veamos; la banca en línea es rentable tanto para los bancos como para los estafadores. En el caso de los estafadores, pueden llevar a cabo campañas de phishing a gran escala de manera económica utilizando la tecnología. Esto les permite llegar a un gran número de posibles víctimas. Además, para evitar ser detectados, recurren a personas conocidas como mulas de dinero. En estos ejemplos, los delincuentes aprovechan las tecnologías de la información y la comunicación para multiplicar sus delitos y aumentar su alcance. Esto no solo hace que los delincuentes sean más culpables, ya que generan más víctimas, sino que también los vuelve más peligrosos. (Hartel, 2023).

La utilización de modelos predictivos de robos basados en patrones de victimización repetidos. Estos modelos tienen como objetivo predecir la ocurrencia de robos utilizando patrones espaciotemporales de riesgo cercanos a los robos iniciales. Aunque se han implementado estos modelos en varios países, los resultados obtenidos no siempre han cumplido las expectativas iniciales, lo que ha llevado a cuestionar su eficacia real. La capacidad de predecir la delincuencia con el fin de mejorar las estrategias policiales preventivas sigue siendo un tema de estudio. El objetivo principal de este estudio es identificar las limitaciones y los éxitos de estos modelos predictivos en el contexto de predecir robos basados en patrones espaciotemporales de riesgo cercanos a robos anteriores. (Boqué et al, 2022).

Los avances recientes en tecnologías de inteligencia artificial (IA) han llevado a un significativo crecimiento en innovación y automatización. Sin embargo, también advierte que estas tecnologías de IA pueden ser utilizadas con fines maliciosos. Un ejemplo específico llamado DeepLocker, que utiliza la IA de manera intencional con fines dañinos y puede evadir sistemas de seguridad. Además, los actores de amenazas en el ámbito cibernético están constantemente mejorando sus estrategias y utilizando técnicas de IA en lo que se denomina ciberataque basado en IA. Estos ataques pueden combinarse con técnicas de ataque convencionales para causar un daño mayor. Pese a los esfuerzos por frenar los ciberataques, no se ha logrado tal finalidad, por lo que se requiere que se presenten defensas efectivas. (Kaloudi y Li, 2020).

La eficacia en la prevención del delito, mediada por la tecnología, puede ser mejorada a través de una mayor adquisición de conocimientos por parte de la comunidad. Una forma de lograrlo sería incrementar el acceso a Internet en todas las ubicaciones. Se propone que los ciudadanos participen en programas locales donde profesionales capacitados, voluntarios y autoridades enseñarían a la comunidad el uso de nuevas tecnologías para prevenir el crimen. Estos esfuerzos involucrarían a departamentos de policía locales y a gobiernos locales para proporcionar información sobre estrategias de prevención del delito a través de herramientas. Por tanto, se requiere la colaboración de partes interesadas clave en áreas como la prevención del delito, el análisis de grandes datos y las tecnologías emergentes. (Stubbs-Richardson et al, 2018).

3. Metodología

La presente investigación optó el tipo de investigación básica. Estas investigaciones se caracterizan por su enfoque en la creación de nuevos conocimientos teóricos que no tienen una conexión directa con problemas prácticos. Su objetivo principal es avanzar en el conocimiento teórico en un campo específico. A diferencia de la investigación aplicada, que se centra en resolver problemas prácticos, la investigación básica busca entender los principios fundamentales y las teorías en una disciplina sin necesidad de aplicaciones inmediatas en mente.

De otro lado, se utilizó el diseño fenomenológico hermenéutico, ya que se busca analizar y dar sentido a datos y discursos cualitativos para abordar un problema a través de los objetivos, el marco teórico, los resultados y, en particular, las experiencias de los participantes. Esto se logra mediante entrevistas que exploran sus creencias, vivencias y otros aportes valiosos que se pueden obtener a través del enfoque fenomenológico.

El enfoque de investigación de este estudio es cualitativo, ya que busca comprender un fenómeno social desde una perspectiva subjetiva, integral y naturalista. El propósito principal no es generalizar resultados, sino interpretar cómo se desarrollan los acontecimientos, desde la perspectiva de los participantes, en el contexto donde ocurren los fenómenos sociales. Para recopilar datos, se utilizarán entrevistas en profundidad no estructuradas. Se empleará un método de muestreo no probabilístico y el análisis de los datos será inductivo, es decir, se llevará a cabo de manera abierta y flexible para lograr una comprensión más profunda de las experiencias de los participantes.

4. Resultados

La exposición de los resultados se ha realizado acorde a los objetivos planteados. En tal sentido, respecto al objetivo general concerniente a determinar de qué manera la zozobra social ha sido condicionada por la pandemia hacia una neo criminalidad, se obtuvo los siguientes resultados.

En relación a la pregunta, ¿La neo criminalidad se modernizó en pandemia con la aparición de nuevas tecnologías?, los entrevistados respondieron:

Calongo: Efectivamente, a raíz de la pandemia y como una medida de bioseguridad, la ciudadanía en general empezó a utilizar la tecnología, particularmente los aplicativos para hacer pedidos y compras online y si bien es cierto, esta medida facilitó el comercio de bienes y servicios; sin embargo, dio lugar también a la aparición de nuevas formas delictivas a través de la tecnología, de allí que, hoy tenemos mayor incidencia en delitos cibernéticos; tales como las estafas informáticas, que consiste en realizar una actividad engañosa produciendo un desplazamiento patrimonial en perjuicio de la víctima y obteniendo así un ánimo de lucro. El phishing, que consiste en la obtención fraudulenta de contraseñas bancarias con el fin de transferir dinero a otra cuenta bancaria y el carding que consiste en un copiado de las tarjetas de crédito de la víctima para realizar posteriormente una adquisición de bienes, entre otras.

León: Las medidas que tomaron muchos gobiernos para limitar el contagio del COVID-19 interrumpieron diferentes eslabones de la cadena criminal. Por ejemplo, las cuarentenas y restricciones a la movilidad redujeron las oportunidades de interacción entre víctimas y victimarios con la excepción de la violencia doméstica, que registró un aumento de casos cuando víctimas y agresores permanecieron confinados en el hogar. También se vieron afectadas las cadenas de suministro de piezas de auto robadas o la venta de drogas ilícitas.

Peña: Efectivamente es un nuevo tipo de criminalidad la cual se ajusta a la globalización, la pandemia de una y/o otra forma debido al confinamiento nos obligó a interactuar con otras personas con las cuales intercambiamos datos y otros tipos de información, permitiendo de esta manera que este nuevo tipo de criminalidad aparezca con el uso de las herramientas tecnológicas.

Uribe: Evidentemente si se ha presentado una modernización de la criminalidad con la aparición de las nuevas tecnologías, durante la pandemia y pos pandemia, pues la criminalidad también hace uso del avance de la ciencia y tecnología para sus propios fines y muchas veces, dispone de mayores recursos que las fuerzas del orden para la adquisición de tecnología de punta y contratación de profesionales de alto nivel competitivo para la máxima explotación de los recursos tecnológicos en aspectos de su interés.

La pandemia también ha tenido impacto en ello, en razón que por razones de salubridad y evitar el contacto personal, un alto porcentaje de actividades, entre ellas, las comerciales, bancarias, educativas, de salud, etc., imperativamente se realizaban a través de medios tecnológicos de información y comunicación, posibilitando un "mercado" para los hackers y delincuentes que usaban dichos medios tecnológicos para materializar sus actividades delictivas. Huamaní: Considero que si se modernizo especialmente en el área informática.

Hinojosa: Efectivamente, con el confinamiento al que todos los ciudadanos fuimos sometidos para evitar la propagación del Covid 19, si bien es cierto los robos a entidades bancarias, personas naturales, así como las estafas entre otros delitos comunes tuvieron una baja considerable y es más me atrevería a decir que durante la pandemia casi no se dieron esos hechos delictivos; sin embargo, los delitos a través de las nuevas tecnologías se incrementaron. Se dieron suplantaciones de identidades, transferencias bancarias mediante la clonación de tarjetas, es decir, se utilizó la tecnología para a través de las mismas incurrir en hechos ilícitos y la policía y fiscalía no se encontró preparada para hacer frente a esas nuevas formas delictivas.

Remigio: La neo criminalidad comprendida como un fenómeno de criminalización moderna, no sufrió un proceso de modernización con la aparición de las nuevas tecnologías en la pandemia, dado que las formas de aparición de la neo criminalidad atraviesan una suerte de proliferación desde las últimas décadas en el mundo, sino que se fortificó reproduciendo formas atípicas de criminalidad bajo el pretexto de diferentes objetivos penales y extrapenales.

Mientras tanto, en relación a la pregunta, ¿Qué entiende Ud. por Neo criminalidad, cree Usted que la aparición de la inteligencia artificial está siendo aprovechada por los delincuentes para cometer actividades ilícitas?, los entrevistados respondieron de la siguiente manera:

Calongo: Son aquellas formas delictivas que son producto de la globalización y el desarrollo de la tecnología, como las estafas informáticas, a diferencia de la delincuencia tradicional violento como el robo que necesitaba la presencia física de la gente y de la víctima para apropiarse de un bien, actualmente se puede hacer a través de la informática; inclusive se habla también de delitos contra la libertad sexual y acoso a través de las redes sociales. Y es en esta línea la inteligencia artificial también está siendo mal utilizada, por ejemplo, para suplantar identidad, superponiéndole un rostro, cabellos, entre otros.

León: Esta investigación realizada tiene como finalidad poder establecer parámetros de tratamiento jurídico respecto del aún novísimo tipo penal del marcaje o reglaje, figura que es parte del siempre cuestionado Derecho Penal del enemigo, como una manera de anteposición a las barreras criminales, siendo ésta una de las figuras muy cuestionadas debido a la sanción que reciben los actos preparatorios.

Peña: Es una nueva criminalidad producto de la globalización del mundo y de uso de las herramientas tecnológicas, teniendo entendido que esta nueva forma de criminalidad utiliza la inteligencia artificial para cometer actos ilícitos en agravio de personas naturales y jurídicas.

Uribe: Neo es un prefijo que significa nuevo y entendemos que el término implica la aparición de una nueva criminalidad que explota los recursos tecnológicos que brinda el avance la ciencia y la tecnología, entre ellos, la tecnología artificial, que indudablemente es utilizada por las organizaciones criminales para el planeamiento, organización y ejecución de actividades criminales, pues ésta, utiliza algoritmos aplicables a cualquier requerimiento de análisis de información demandado por la criminalidad.

Huamaní: Entiendo por Neo criminalidad, como la aparición de nuevas formas de criminalidad, y con respecto a la aparición de la inteligencia artificial, considero que, si estaría siendo aprovechado, y como siempre la aparición de nuevas tecnologías es usada para bien y para mal.

Hinojosa: Por neo criminalidad se entiende las nuevas formas de criminalidad que, a raíz de la virtualidad como consecuencia de la pandemia, originó el establecimiento de organizaciones transnacionales dedicadas a cometer hechos ilícitos a través de herramientas tecnológicas. Se agrega que la inteligencia artificial sirve de apoyo a los delincuentes, puesto que mediante la imitación de la voz pueden estafar a ciudadanos a través de dispositivos de mayor uso.

Remigio: Conforme lo expusimos en la pregunta anterior, la neo criminalidad es un fenómeno criminológico que consiste en la aparición de nuevas y/o modernas formas de criminalidad en las diferentes esferas delictivas que consisten en rediseñar las añejas fórmulas o teorías del derecho penal para buscar una manera de readaptar el derecho a la modernidad. En cuanto la aparición de la inteligencia artificial como fuente aprovechada de la delincuencia, considero que solo es un móvil más del incremento o aprovechamiento de la criminalidad, dado que la máxima progresiva que la delincuencia avanza en función del avance de la sociedad, se replica en la figura de la inteligencia artificial como cualquier mecanismo que impulse la ola delincuencial en el mundo.

Respecto del primer objetivo específico consistente en analizar cómo facilita el empleo de herramientas tecnológicas en estafas y extorciones generando zozobra en la sociedad, se obtuvieron los siguientes resultados:

Respecto de la pregunta ¿De qué manera Ud. considera, que se puede hacer en caso de recibir extorciones o amenazas con fotos que nunca se vio?, los participantes contestaron de la siguiente manera: Calongo: En primer lugar, las herramientas tecnológicas facilitan hacer, por ejemplo, Photoshop Online, la primera recomendación que se debe hacer es advertir a los ciudadanos que usen claves para sus teléfonos y no debe de ser compartidos a nadie; de datos privados, teniendo en cuenta que hoy por hoy el teléfono móvil es el almacenamiento de datos privados familiares que fácilmente pueden ser empleados por ciberdelincuentes. Una recomendación adicional es el cambio inmediato de teléfono para frustrar el accionar del extorsionador.

León: Es muy fácil crearse una cuenta falsa en Facebook, Gmail, Twitter, Skype, WhatsApp y demás redes sociales. A través de estas cuentas falsas, normalmente creadas en sitios remotos, los extorsionadores agregan a las víctimas y recaudan datos sobre estas para calcular su delito. Por lo que debemos prevenir y tener mucho cuidado con los perfiles que aceptamos como contacto. Por lo que se recomienda no publicar fotos y videos por estas redes sociales, que muchas veces los delincuentes se aprovechan de esto.

Peña: Tenemos que esta nueva forma de usurpación de identidad viene tomando forma en la región de Latinoamérica, para cual utilizan tecnología de punta, un caso reciente fue de una alumna de un colegio en la cual utilizaron sus imágenes de sus páginas sociales con la finalidad de recrear situación de connotación sexual, en ese sentido se debe tener un mayor cuidado en cuanto a las publicaciones que realizamos en las redes sociales, debemos tener mayor seguridad en cuanto a nuestro entorno informático.

Uribe: Se refiere al proceder de la víctima en caso de ser objeto de extorsiones o amenazas por parte de bandas criminales. En esa perspectiva, creemos importante proceder a la denuncia respectiva a la PNP para la realización de un trabajo especializado, pero también, adoptar medidas de seguridad individual y familiar durante sus desplazamientos y en su domicilio.

Huamaní: Considero que frente a este tipo de amenazas se debe tomar todas las medidas necesarias, dado que no existe una sola respuesta para este tipo de delitos y amenazas que causan una gran zozobra en la sociedad.

Hinojosa: De manera inmediata se debe comunicar el hecho a la policía para que a través de la unidad especializada asuma la investigación del caso, con la dirección de la Fiscalía, dado que estas amenazas se realizan a través del wasap, redes sociales, etc., por lo que es necesario tener orden de interceptar llamadas, mensajes, para identificar a los autores del hecho criminal.

Remigio: La lucha contra la delincuencia debe encuadrarse en períodos de políticas criminales, esto es denominado como un antes, durante y después del delito. En ese sentido, los criterios o actuaciones estrictas para combatir la delincuencia artesanal y/o modernizada deben reflejarse en el proceder de las autoridades involucradas con la criminalización, para efectos de reforzar, planificar, estructurar, ampliar, estrategias de lucha contra la delincuencia.

La segunda pregunta fue, ¿Qué hacer si accedió a un contenido falso creado por inteligencia artificial y le robaron los datos personales?, los entrevistados respondieron de la siguiente manera:

Calongo: Actualmente existe la división de alta tecnología de la policía nacional para que puedan acudir y registrar su denuncia y puedan bloquear el uso indebido de sus datos, sin perjuicio de comunicar inmediatamente a la entidad bancaria en caso de tener tarjeta de débito o crédito, así como la empresa de telefonía para el bloqueo del teléfono.

León: En este sentido, como siempre recomendamos, evita compartir en Internet datos personales sensibles como el nombre completo, la dirección, el número de teléfono, fecha de nacimiento, número de la seguridad social o cualesquiera datos que pueda identificarte únicamente.

Peña: Debemos tratar de evitar recibir mensajes o anuncios que de forma imprevista o desconocida son enviadas en nuestras redes sociales, si somos víctimas del robo de datos debemos cancelar la cuenta, tratar de bloquear y advertir a sus allegados la forma y circunstancias en que llego este contenido falso para evitar que otras personas caigan en el mismo error.

Uribe: Bloqueo inmediato de todas las cuentas personales y posteriormente, modificar las claves y mecanismos de seguridad. Huamaní: Una vez tomado el conocimiento, acudir a la Policía Nacional no solo para denunciar el hecho ilícito, sino principalmente para modificar o anular los claves o contraseñas.

Hinojosa: Esto es un tema muy delicado, dado que se accedió al contenido falso y robaron los datos personales, quien lo hizo (robo) pensara que son datos reales y en base a ellos podría iniciar algún tipo de extorsión; en ese caso también se debe dar cuenta a la policía para la investigación del caso si se tuviera alguna evidencia, pero si se pierde y no hay alguna evidencia, ello dificultara la intervención de la fiscalía y policía.

Remigio: Inmediatamente acudir a la autoridad especializada, tal como la policía de la Unidad de Alta Tecnología o la Unidad de Delitos Informáticos. Así como al Ministerio Público especializado en Delitos Informáticos.

La tercera pregunta fue, ¿Que se puede hacer si los delincuentes están usando videos públicos, siendo manipulados para campañas de extorción?, los entrevistados respondieron de la siguiente manera: Calongo: Igualmente denunciar ante la división de alta tecnología de la PN especializados en delitos informáticos que tiene conocimiento sobre Ciberataques.

León: Es necesario renovar periódicamente el soporte de tarjeta bancaria, pues los ciberdelincuentes utilizan bases de datos de números de tarjetas antiguas, desactivar la opción de compras por internet y activarla al efectuar compras de naturaleza digital, no proporcionar información confidencial al recibir llamadas telefónicas de personas que indican ser trabajadores de alguna entidad financiera, no entregar la tarjeta de crédito o débito al momento de realizar compras en comercios, por el contrario, exigir que el pago se efectúe en su presencia.

Peña: En primera instancia tratar de bloquear, la página de donde proviene, luego investigar en cuanto a la forma y circunstancias en que fueron manipulados estos videos, no pagar el dinero que exigen los delincuentes y poner en alerta a las autoridades para que realicen las indagaciones del caso.

Uribe: Creemos que en la actualidad toda persona tiene que tener una actitud de permanente alerta y duda para acceder a páginas, correos o videos públicos o privados, debiendo aplicar un protocolo de seguridad que le permita asegurarse o le garantice que las páginas, correos o videos a los cuales accede sean auténticos, pues en la actualidad, es muy común la clonación de éstos para “piratear” información personal de los usuarios.

Hinojosa: En ese caso concreto, comunicar el hecho a la plataforma de internet para que proceda a bloquear el contenido y además siendo los mismos utilizados para la extorsión, se debe denunciar al hecho a la policía nacional.

Remigio: De igual forma que la pregunta anterior, debemos comunicar a las autoridades especializadas en la materia con el propósito que limiten la propagación de esta información.

Por último, entorno al segundo objetivo específico respecto a identificar cómo afecta el robo de identidad para cometer fraudes financieros en nombre de la víctima, se tuvo lo siguiente:

En lo referido a la pregunta, ¿Qué hacer si fuiste victima por los delincuentes con sofisticados mensajes de voz falsificados para sorprender y cometer el fraude y la extorción?, los entrevistados respondieron:

Calongo: No responder los mensajes y denunciar inmediatamente la policía y cambiar de teléfono

León: En primer lugar, deberás prestar atención al tono de la misma voz. Si ha sido generada con IA, notarás que se parecerá a la de un robot. Lo mejor es que dudes de antemano y escribas de inmediato por una plataforma de confianza y en el mismo momento al supuesto interlocutor.

Peña: No tenemos un formato o forma de abordar estas situaciones ya que se trata de una nueva e innovadora forma de criminalidad que es uy difícil de poder identificar las rutas de donde proviene.

Uribe: Esto es muy usual en estos días, por lo tanto, es importante que a nivel familiar se mantenga permanente contacto para saber la ubicación de cada miembro de la familia y evitar ser sorprendidos por dichos delincuentes. Creo que solamente hay que colgar y nunca brindar ningún dato personal ni familiar a través del teléfono.

Huamaní: Una de las medidas importante es no tomar una decisión inmediata sino después de un tiempo de indagación, pues la voz de algún familiar puede ser grabada o parecida, y de esa forma pueden tratar de extorsionar.

Hinojosa: Así el mensaje de voz sea falsificado, el hecho ilícito está ahí, es decir, la extorsión está ocurriendo y por lo tanto debe denunciarse el hecho para las investigaciones correspondientes.

Remigio: En estos casos la recomendación es realizar la denuncia respectiva señalando fielmente los hechos, asimismo, recomendamos siempre custodiar las evidencias necesarias a fin de no perder ninguna de ellas, mucho menos manipularlas para de esta manera las autoridades realicen un trabajo más elaborado en la persecución de estos delitos.

La segunda pregunta fue, en su experiencia ¿Considera Ud. que el estado debe implementar tecnología de punta para detectar a tiempo estos tipos de fraudes financieros que son a través de la inteligencia artificial? ¿Cómo prepararse para detectar la voz falsificada?, los entrevistados respondieron de la siguiente manera:

Calongo: Es responsabilidad del Estado garantizar la seguridad de los ciudadanos, en este caso los delitos que se dan a través de la informática; y desarrollar toda una campaña nacional de sensibilización a la población de mayor seguridad en el uso de teléfonos y claves para el uso de las tecnologías.

León: El estado debe realizar un proceso que, tradicionalmente, las entidades han llevado de forma totalmente manual, lo que puede ser lento, costoso y propenso a errores. Y aquí es donde la IA puede desempeñar un papel importante para ayudar a solucionar estos desafíos.

Por un lado, porque la IA puede automatizar gran parte del proceso para conocer clientes, utilizando algoritmos para recopilar, verificar y analizar la información relevante de los clientes. También porque mejora la precisión de los controles de las actividades del posible cliente al reducir errores humanos y sesgos, lo que ayuda a las instituciones financieras a cumplir con los requisitos regulatorios de manera más rápida y eficiente, lo que a su vez mejora la experiencia del cliente al reducir los tiempos de espera.

Peña: El estado es el encargado de cuidar al ciudadano mediante el derecho penal, pero este DP de esta a la par con esta nueva forma de criminalidad para cual debe especializar a las agencias de control social a través de la policía y el ministerio público o fiscalías especializadas en ciberdelincuencia, asimismo debe dictar normas preventivas y reguladoras sobre el uso de IA.

Uribe: Indudablemente que sí no se dispone de estos recursos, los delincuentes tendrán una ventaja comparativa respecto a las fuerzas del orden, pues como ya lo hemos mencionado, muchas organizaciones criminales usan tecnología de vanguardia y profesionales de alto nivel competitivo para emplearlos en sus actividades delictivas.

Huamaní: Considero que cualquier medida o uso de tecnología de punta que pueda erradicar o al menos mitigar considerablemente este delito es una buena estrategia que debe aplicar el Estado.

Hinojosa: Para todos los delitos cibernéticos, es decir aquellos que se comenten a través de las herramientas de internet, que puede ser violándose el correo electrónico, el wasap, el número celular y la utilización de la voz a través de la la inteligencia digital, es necesario que el estado repotencie a la fiscalía y a la policía, proporcionando material logístico de última generación; que el juez acceda al levantamiento de las comunicaciones en tiempo reducido para que se utilice esa herramientas y se acceda a la comunicación entre los delincuentes, conversaciones con el extorsionado, etc. y así se pueda actuar de manera rápida y eficiente.

Remigio: Definitivamente no todos los países y sobre todo el Perú no dispone de Tecnología moderna y estrictamente el sector del interior no cuenta con la tecnología destacada y necesaria para combatir la aparición de las conductas delictivas que surgen de la propagación de la tecnología e inteligencia artificial. Esta situación es imprescindible solucionarla para cumplir con los objetivos de lucha contra la delincuencia.

Finalmente, la preparación para detectar los diferentes signos de falsedad y criminalidad son inmediatamente necesarios dado que la delincuencia se acrecienta conforme la sociedad evoluciona.

La tercera pregunta fue, ¿La policía está capacitada para detener y evitar abrir cuentas a nombre de la víctima?, los entrevistados respondieron de la siguiente manera:

Calongo: En mi experiencia considero que aún no. Además, este es un tema que debe en primer lugar ser visto por las entidades bancarias, es decir para extremar las medidas de seguridad para la apertura de cuentas, actualmente algunos bancos Online, apertura cuentas, que por cierto genera un alto riesgo de suplantación.

León: La Policía Nacional del Perú está preparada para detener y evitar este tipo de delitos, gracias a sus unidades especializadas en combatir la misma, asimismo hay denuncias sobre los atacantes que emplearon herramientas digitales como redes sociales, software y otras plataformas en línea. En esta categoría hubo 268 denuncias en el 2019, mientras que el año previo hubo 362 registros. El acoso sexual, las estafas en línea, amenazas desde mensajería o redes sociales o la extorsión agrupan la mayor cantidad de denuncias.

Peña: No está capacitada, por cuanto no cuenta con la tecnología requerida para afrontar a esta nueva versión de criminalidad.

Uribe: Actualmente la PNP dispone de una Unidad Especializada de Alta Tecnología que trabaja en actividades de esa naturaleza; sin embargo, no me es posible afirmar o negar si los efectivos que prestan servicios en dicha unidad, disponen de tal capacitación, pues no tengo contacto cercano con ellos; sin embargo, puedo presumir que no la tienen.

Huamaní: La Policía debe tener una capacitación tecnológica adecuada para combatir la ciberdelincuencia, pero también capacitar en el ámbito moral- ética, dado que por el involucramiento en los delitos de algunos malos elementos la sociedad pierde confianza en la Policía.

Hinojosa: La policía podría estar preparada, pero si la fiscalía actúa lento en obtener el levantamiento del secreto bancario, cuando se hace el dinero ya fue redirigido a otra cuenta y así sucesivamente. Para el tema de la apertura de las cuentas, debería ser exigencia que las mismas se activen con la presencia física de la persona que solicita el servicio, ningún trámite para apertura de cuenta, debe ser canalizado por internet.

Remigio: Las autoridades no pueden limitar la creación de información falsificada o fraguada, esto es un imposible técnico y jurídico. Empero, si pueden combatir su proliferación en diferentes estratos, así como la lucha para castigar los comportamientos delictivos que sostengan estos hechos.

La cuarta pregunta fue, ¿La alta tecnología de la Policía está preparada para evitar crear información engañosa y actividades ilegales?, los entrevistados respondieron de la siguiente manera:

Calongo: Considero que sí, a pesar de sus limitaciones, en la actualidad se viene empleando la figura del agente encubierto informático, quien va ingresando y revisando las páginas web y redes sociales para detectar organizaciones criminales vinculadas al tráfico ilícito trata de personas y delincuencia entre otros delitos.

León: La Dirección de Tecnología de la Información y Comunicaciones, es el órgano de apoyo especializado en tecnologías de la información y comunicaciones responsable de administrar, organizar, dirigir, coordinar, ejecutar y controlar las actividades para la implementación de las tecnologías de información y comunicaciones necesarias que den soporte a la función policial, en el marco de los lineamientos dictados por el Ministerio del Interior y las disposiciones del Director General de la Policía Nacional del Perú.

Peña: Volvemos a indicar que no cuenta con la tecnología debida para realizar las investigaciones a esta nueva e innovadora criminalidad. Uribe: Es poco probable que la PNP tenga la preparación y medios para evitar crear información engañosa, pues esta puede ser creada por cualquier persona del país o extranjero, por lo tanto, la probabilidad de cobertura y alcance para evitar dichas actividades, es muy baja.

Huamaní: Considero que no, pero en la actualidad por la alta incidencia de delitos de suma gravedad el Estado tendrá que implementar, como política de gobierno de seguridad social, la adquisición y el uso de alta tecnología.

Hinojosa: Si bien tiene una buena preparación, se debe tener en cuenta que los delincuentes están a la vanguardia de las tecnológicas, por lo que urge un trabajo coordinado entre la Fiscalía-PNP y el Poder Judicial.

Remigio: Las autoridades no pueden limitar la creación de información falsificada o fraguada, esto es un imposible técnico y jurídico. Empero, si pueden combatir su proliferación en diferentes estratos, así como la lucha para castigar los comportamientos delictivos que sostengan estos hechos.

5. Discusión

El objetivo general ha consistido en determinar de qué manera la zozobra social ha sido condicionada por la pandemia hacia una neo criminalidad, los autores Odilla (2023) y Buil-Gil et al (2021) afirmaron que, durante la pandemia de COVID-19, los primeros confinamientos provocaron cambios en las actividades diarias de las personas, lo que afectó las tasas de delincuencia, lo que ha conllevado que los delitos en línea aumenten. A su turno Trinidad et al (2021) y Junger et al (2020) sostuvieron que se ha investigado poco sobre la relación entre los confinamientos sucesivos y su impacto a medio plazo en la delincuencia, y hay pocos estudios que comparen las tendencias de delitos en línea y fuera de línea utilizando el mismo conjunto de datos.

Los participantes Calongo (2023), Peña (2023), Uribe (2023) y Remigio (2023), coincidieron que la neo criminalidad se refiere a nuevas formas de criminalidad que han surgido como resultado de la globalización y el uso de

herramientas tecnológicas. Estas formas de criminalidad incluyen estafas informáticas, delitos contra la libertad sexual y acoso a través de las redes sociales, entre otros.

León (2023) y Remigio coincidieron que, la inteligencia artificial está siendo aprovechada por los delincuentes para cometer actividades ilícitas. La inteligencia artificial se utiliza para suplantar identidades, superponer características físicas en imágenes y videos, y cometer estafas a través de dispositivos de comunicación. La tecnología artificial proporciona a las delincuentes herramientas para planear y llevar a cabo actividades criminales de manera más efectiva.

Lo señalado por los autores y entrevistados conlleva afirmar que la tecnología ha dado lugar a nuevas oportunidades para la criminalidad, y es importante que las autoridades y la sociedad en su conjunto estén preparadas para hacer frente a esta neo criminalidad y proteger a las posibles víctimas.

En relación al primer objetivo específico, que ha consistido en analizar cómo facilita el empleo de herramientas tecnológicas en estafas y extorciones generando zozobra en la sociedad se obtuvo lo siguiente:

Los autores Halford (2020) y Lwin y Birks (2023) centraron sus ideas en el sentido que, En cuanto a los cambios en los niveles de delincuencia durante la pandemia de COVID-19, se ha observado un aumento en la delincuencia cibernética, el fraude y otros delitos emergentes, ya que la pandemia ha creado nuevas oportunidades delictivas. Por tanto, sugirieron que las políticas y prácticas centradas en la reducción de oportunidades delictivas pueden tener un impacto positivo en la reducción de la delincuencia, especialmente entre los jóvenes. Al reducir las oportunidades para cometer delitos, se puede desalentar la participación en actividades delictivas. Esto destaca la importancia de abordar la prevención y la reducción de oportunidades en la lucha contra la delincuencia, especialmente en el contexto de la delincuencia cibernética y las estafas.

Respecto a este objetivo, los participantes, Hinojosa (2023), Remigio (2023) y Huamaní (2023) sostuvieron que con la finalidad de evitar las estafas y extorciones yace la necesidad de la protección de información personal, es decir, evitar compartir en línea datos personales confidenciales que puedan ser utilizados para identificarlo de manera única. Peña (2023, León (2023) y Colongo (2023) agregaron la importancia de la gestión de contactos en redes sociales, es decir, ser precavido al aceptar solicitudes de amistad en plataformas de redes sociales y al publicar fotografías y videos en línea, ya que los delincuentes pueden aprovechar esta información para llevar a cabo actos de extorsión.

Por último, respecto al segundo objetivo que ha consistido en identificar cómo afecta el robo de identidad para cometer fraudes financieros en nombre de la víctima se obtuvo lo siguiente: Los autores, Stottelaar (2014) y Lwin y Birks (2023) indicaron que, la exposición de información personal en línea puede aumentar la vulnerabilidad de las personas a ser víctimas de delitos. Al compartir detalles específicos sobre su ubicación y actividades en redes sociales y otras plataformas en línea, las personas pueden estar proporcionando a los delincuentes información valiosa que podría utilizarse para perpetrar delitos. En tal sentido, la publicación de información sobre ubicación y actividades en tiempo real en las redes sociales, puede facilitar a los delincuentes el seguimiento y la predicción de los patrones de actividad de una persona, por tanto, es esencial que las personas sean conscientes de los riesgos asociados con la exposición excesiva de información personal en línea y tomen medidas para proteger su privacidad y seguridad.

Los participantes, Hinojosa (2023), Uribe (2023) y Calongo (2023), indicaron que yace la necesidad que el Estado desarrolle campañas de sensibilización para promover la seguridad en el uso de teléfonos y tecnologías. Así como también se deben especializar en la lucha contra la nueva forma de criminalidad y dicten normas preventivas y reguladoras sobre el uso de la inteligencia artificial. A su turno, Remigio (2023), Peña (2023) y León (2023) sostuvieron que la inteligencia artificial puede desempeñar un papel importante en la detección de fraudes financieros, automatizando los procesos que conlleven a la lucha contra el robo de información personal.

6. Conclusiones

El empleo de herramientas tecnológicas en estafas y extorciones ha generado zozobra en la sociedad en la medida que la ”neo criminalidad”hace referencia a las nuevas manifestaciones delictivas que han surgido como consecuencia de la globalización y el empleo de herramientas tecnológicas. Estas formas de delincuencia comprenden un amplio espectro de actividades, como el fraude informático, robo de identidad, suplantación entre otros. La inteligencia artificial ha adquirido un papel fundamental en el arsenal de los delincuentes para llevar a cabo estas actividades ilícitas. En ese sentido, los delincuentes hacen uso de la inteligencia artificial en la ejecución de diversas actividades criminales. Ejemplos de cómo se emplea la inteligencia artificial en el ámbito del crimen incluyen la suplantación de identidades, dado que la inteligencia artificial es empleada por los delincuentes para generar perfiles ficticios en línea y asumir identidades ajenas con propósitos fraudulentos. Del mismo modo, la manipulación de imágenes y videos, es decir, la inteligencia artificial se utiliza para sobreponer características físicas en imágenes y grabaciones, lo cual puede resultar en la creación de contenido falso o alterado. Así también, las estafas a través de medios de comunicación, en donde los delincuentes pueden aprovechar la inteligencia artificial para llevar a cabo estafas por

medio de mensajes de voz falsos o mensajes de texto engañosos, engañando a las víctimas y obteniendo información personal o financiera. En líneas generales puede advertirse que, la tecnología artificial otorga a los delincuentes herramientas avanzadas para planificar y ejecutar sus actividades delictivas de manera más eficaz, planteando así nuevos desafíos tanto para las autoridades como para la sociedad en su conjunto en su lucha contra esta forma de delincuencia en constante evolución. Por tanto, la prevención y la preparación tecnológica son esenciales para enfrentar estos desafíos y salvaguardar a las personas de las actividades criminales basadas en la inteligencia artificial.

7. Referencias bibliográficas

Boqué, P., Saez, M. y Serra, L. (2022). Necesidad de ir más allá: utilizar INLA para descubrir límites y posibilidades de predicción espaciotemporal de robos en entornos heterogéneos. Ciencia del crimen, 11 (7).

Buil-Gil, D., Zeng, Y. y Kemp, S. (2021). La delincuencia fuera de línea vuelve a los niveles anteriores a COVID, la cibernética se mantiene alta: análisis de series temporales interrumpidas en Irlanda del Norte. Ciencia criminal, 10 (26).

Caldwell, M., Andrews, J. y Tanay, T. (2020). Crimen futuro habilitado por IA. Ciencia del crimen, 9 (14).

Farrell, G. y Birks, D. (2018). ¿El ciberdelito provocó la caída del crimen? Ciencia del crimen, 7 (8).

Halford, E., Dixon, A. y Farrell, G. (2020). Crimen y coronavirus: distanciamiento social, encierro y elasticidad de la movilidad del crimen. Ciencia del crimen, 9 (11).

Hartel, P., Wegberg, R. y Van Staalduinen, M. (2023). Investigación de la gravedad de la sentencia con datos judiciales abiertos. Eur J Crim Policy Res, 29, pp. 579–599.

Hartel, P. y Van-Wegberg, R. (2023). ¿Se está oscureciendo? Analizar el impacto del cifrado de extremo a extremo en el resultado de los casos de los tribunales penales holandeses. Ciencia del crimen, 12 (5).

Junger, M., Wang, V. y Schlömer, M. (2020). Fraude contra empresas tanto en línea como fuera de línea: guiones de delitos, características comerciales, esfuerzos y beneficios. Ciencia del crimen, 9 (13).

Kaloudi, N. y Li, J. (2020). El panorama de las ciberamenazas basadas en IA: una encuesta. Revistas ACM, 53 (1).

Lwin, Z. y Birks, D. (2023). Respaldo del análisis de guiones criminales de estafas con procesamiento de lenguaje natural. Ciencia del crimen 12 (1).

Miró-Llinares, F. y Moneva, A. (2019). ¿Qué pasa con el ciberespacio (y el ciberdelito junto con él)? Una respuesta a Farrell y Birks "¿El ciberdelito provocó una disminución del crimen?". Ciencia del crimen, 8 (12).

Newton, A. y Felson, M. (2015). Patrones delictivos en el tiempo y el espacio: la dinámica de las oportunidades delictivas en las zonas urbanas. Ciencia del crimen, 4 (11).

Odilla, F. (2023). Bots against corruption: Exploring the benefits and limitations of AI-based anti-corruption technology. Crime Law Soc Change, 80, pp 353–396.

O'Hara, A., Ko, R. y Mazerolle, L. (2021). Análisis del guión del crimen para abuso sexual basado en imágenes de adultos: un estudio de los puntos de intervención criminal para delincuentes del estilo de retribución. Ciencia del crimen, 9 (26).

Reep-van, C. y Junger, M. (2018). Víctimas del cibercrimen en Europa: una revisión de las encuestas a víctimas. Ciencia del crimen, 7 (5).

Stambøl, E. y Solhjell, R. (2021). Embodiments and frictions of statehood in transnational criminal justice. Theoretical Criminology, 25 (3), pp. 493-510.

Stottelaar, B., Senden, J. y Montoya, L. (2014). Las redes sociales deportivas online como facilitadoras del delito. Ciencia del crimen, 3 (8).

Stubbs-Richardson, M., Cosby, A. y Bergene, K. (2018). Buscando seguridad: prevención del delito en la era de Google. Ciencia del crimen, 7 (21).

Trinidad, A., Vozmediano, L., Ocáriz, E. y San-Juan, C. (2021). Taking a Walk on the Wild Side": Exploring Residence-to-Crime in Juveniles. Crime & Delinquency, 67 (1), pp. 58-81.

Van-Gelder, J., Otte, M. y Luciano, E. (2014). Uso de la realidad virtual en la investigación criminológica. Ciencia del crimen, 3 (10).