

Tecnología, captación y explotación: La nueva frontera en la lucha contra la trata de personas

ARTÍCULO EN PRENSA

Technology, recruitment and exploitation: The new frontier in the fight against human trafficking

ARTICLE IN PRESS

Daniel Romera Mejías 

Universidad de Sevilla. España

dromera@us.es

ORCID: <https://orcid.org/0009-0008-8284-4851>

Waldimeiry Correa da Silva 

Universidad de Sevilla. España

wcorrea@us.es

ORCID: <https://orcid.org/0000-0002-1863-8454>

<https://doi.org/10.18543/djhr.3617>

Fecha de recepción: 09.10.2025

Fecha de aceptación: 06.07.2026

Fecha de publicación en línea: julio 2026

Cómo citar / Citation: Romera, Daniel y Waldimeiry Correa. 2026. «Tecnología, captación y explotación: La nueva frontera en la lucha contra la trata de personas». *Deusto Journal of Human Rights*. <https://doi.org/10.18543/djhr.3617>

Sumario: 1. Consideraciones iniciales: la evolución de la TP en el entorno digital. 2. Las nuevas tecnologías y su relación con la trata. 2.1. Evolución del uso de Internet: La web 3.0 y la automatización del delito. 2.2. La importancia de la *dark web* y las plataformas digitales en las redes de trata. 2.3. El uso de la IA en el control y explotación de las víctimas. 3. Herramientas tecnológicas en la lucha contra la trata digital. 3.1. *Traffik Analysis Hub*: mapeo de redes de trata. 3.2. PhotoDNA: Identificación de material de explotación. 3.3. *Traffic Jam*: Análisis de datos forenses. 3.4. *Spotlight* y *TraffickCam*: Inteligencia artificial en la identificación de ubicaciones y víctimas. 4. Limitaciones legales y cooperación internacional en el desarrollo de tecnología contra la trata de personas. Consideraciones finales. Referencias.

Resumen: Este estudio analiza el impacto del desarrollo tecnológico y la inteligencia artificial (IA) en la trata de personas (TP), considerando su incidencia en los métodos de captación, explotación y evasión, así como en las contramedidas adoptadas para combatirla. El artículo aborda la evolución de la TP en entornos digitales, el uso de tecnologías emergentes, las estrategias de lucha contra la trata digital y los dilemas éticos del empleo de IA. La metodología empleada se basa en una revisión narrativa cualitativa, permitiendo examinar el estado de la cuestión y analizar este fenómeno desde una perspectiva crítica. La investigación se sitúa en la intersección entre la TP y el impacto de la IA, tanto en su expansión como en su combate.

Palabras clave: Derechos humanos, ética, inteligencia artificial, trata de seres humanos, trata digital.

Abstract: This study analyzes the impact of technological development and artificial intelligence (AI) on human trafficking (HT), considering its influence on recruitment, exploitation, and evasion methods, as well as on the countermeasures adopted to combat it. The article examines the evolution of HT in digital environments, the use of emerging technologies, strategies to fight digital trafficking, and the ethical dilemmas involved in the use of AI. The methodology is based on an literature qualitative analysis, allowing for an assessment of the state of the art and a critical analysis of this phenomenon. The research is situated at the intersection of HT and the impact of AI, both in its expansion and in the efforts to combat it.

Keywords: Human rights, ethics, artificial intelligence, human trafficking, digital trafficking.

1. Consideraciones iniciales: la evolución de la TP en el entorno digital¹

El Protocolo de Palermo² (2000) ofrece un marco jurídico internacional que explica lo que se entiende por trata de personas (TP). Esta definición se fundamenta en la captación, el transporte, el traslado, la acogida o la recepción de personas, a través de diferentes medios coercitivos, violentos, fraudulentos o engaños, mediante el abuso de situación de vulnerabilidad, con el propósito de explotar a una persona (art. 3). Este marco jurídico debe ser interpretado como un proceso derivado de la conjunción de tres elementos constitutivos interrelacionados: una acción, los medios y la finalidad de explotación directa o indirecta de la persona (Correa da Silva 2018). De ahí, que se considere una noción jurídica compleja (Shelley 2010), relacional (Correa da Silva 2018) y que involucra diferentes categorías jurídicas, como la migración, la explotación (sexual o laboral), las formas contemporáneas de esclavitud y otros delitos conexos³.

La TP se origina en virtud de varios problemas sociales, políticos, medioambientales y económicos que se afectan mutuamente de una manera compleja. Respecto a los perfiles de vulnerabilidad, existen factores recurrentes como pobreza, discriminación de género, conflictos armados, desastres naturales y desplazamientos forzados (UNODC 2024, Shelley 2010). La intersección de múltiples vulnerabilidades aumenta significativamente el riesgo: mujeres migrantes indocumentadas, minorías étnicas marginadas, personas LGBTQ+ rechazadas por sus familias y comunidades y niños sin cuidados parentales adecuados son grupos que enfrentan riesgos desproporcionados (UNODC 2024). Es por ello que la comprensión sobre la TP exige una visión interseccional que permita entrever su

¹ Este artículo forma parte de los resultados del proyecto de investigación CNS2023-144884. Ambos autores han contribuido de manera equitativa a la concepción, investigación y redacción del presente trabajo.

² ONU. AG RE55/25/2000. Protocolo para prevenir, reprimir y sancionar la trata de personas, especialmente mujeres y niños, que complementa la Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional. Actualmente ratificado por 178 países.

³ A nivel regional, diversos instrumentos han reforzado este marco. En el ámbito europeo, el Convenio del Consejo de Europa sobre la lucha contra la trata de seres humanos introduce mecanismos de supervisión y enfatiza la necesidad de garantizar la asistencia y protección efectiva de las víctimas (Instrumento de Ratificación del Convenio del Consejo de Europa sobre la lucha contra la trata de seres humanos, Convenio n. 197 del Consejo de Europa). Este enfoque resulta particularmente relevante en entornos digitales, donde las formas de explotación pueden ser menos visibles pero igualmente lesivas.

carácter estructural, donde se sobreponen la pobreza, la raza/etnia, la movilidad humana, el género, las discriminaciones y las situaciones de amenaza a la seguridad humana, contribuyendo así a perpetuar situaciones de injusticia social (Correa da Silva 2018).

La UNODC (2024) identifica tres niveles principales de operación: pequeñas redes informales, grupos criminales de tamaño medio con cierta especialización, y organizaciones criminales complejas con operaciones transnacionales y múltiples actividades ilícitas. Se infiere que las redes de trata presentan estructuras organizativas diversas que varían desde individuos oportunistas hasta organizaciones criminales transnacionales altamente sofisticadas (Lazarus et al. 2025). La UNODC (2024) ha identificado más de 500 flujos de trata distintos a nivel mundial, demostrando la extraordinaria adaptabilidad de este delito a diferentes contextos y la necesidad de respuestas coordinadas internacionalmente. Dado este carácter trasnacional se demanda una coordinada cooperación internacional.

La explotación también ha migrado parcialmente al entorno digital debido al desarrollo de las tecnologías y permeabilidad de las fronteras, la llamada trata digital o “trata cibernética” (Lazarus et al. 2025). El Grupo Interinstitucional de Coordinación contra la Trata de Personas ha documentado el auge de formas de explotación sexual en línea como pornografía forzada, actuaciones sexuales vía webcam y producción de material de trata. Los delincuentes usan estrategias en línea sofisticadas para engañar a las víctimas, quienes cruzan fronteras sin saberlo a países con leyes laxas, facilitando la explotación.

A estas tácticas, la UNODC añade otras dos estrategias habituales utilizadas por los tratantes para engañar y captar víctimas: la “caza” y la “pesca”⁴. Se considera que la “caza” requiere un uso intensivo de ingeniería social personalizada, mientras que la “pesca” se apoya en la automatización algorítmica para captar perfiles vulnerables a gran escala, transformando la captación en un proceso de marketing ilícito altamente eficiente (Hendrik 2018). A su vez, afirma que las plataformas en línea ayudan a los tratantes a buscar de forma proactiva y anónima un tipo específico de persona que consideren especialmente susceptible de favorecer su plan (el proceso de caza), o a atraer pasivamente a posibles víctimas publicando en línea y esperando

⁴ Aunque en la literatura reciente se ha revalorizado la distinción entre *hunting* y *phishing* en entornos digitales, estos patrones de captación no son novedosos. Informes previos de la Oficina de Drogas y Crimen de Naciones Unidas ya identificaban estrategias diferenciadas de captación directa e indirecta en contextos online y offline, posteriormente desarrolladas por diversos autores en el análisis de la trata facilitada por tecnologías digitales.

una respuesta (el proceso de pesca) (UNODC 2020 y 2024). Una vez identificadas las víctimas potenciales y establecido el contacto, la comunicación a través de Internet sirve como una poderosa herramienta para engañar a las personas con falsas promesas de educación, empleo, vivienda o relaciones románticas solo para atraerlas a situaciones de trata laboral y sexual. Estas modalidades permiten a los explotadores acceder a mercados globales mientras mantienen a las víctimas en ubicaciones controladas, reduciendo riesgos de detección.

Lazarus et al. (2025) explican cómo los ciberdelincuentes utilizan tácticas de reclutamiento engañosas y plataformas digitales para atrapar y explotar a las víctimas de la TP en el contexto del cibercrimen. Los autores sostienen que existe una relación bidireccional entre la TP y el cibercrimen, donde los delincuentes no solo explotan a las víctimas para cometer fraudes en línea, sino que también utilizan el ciberespacio para reclutar y controlar a estas personas. En consonancia con esto Sarkar y Shuka (2024), explican que el ciberdelito no solo conduce al tráfico físico de víctimas, sino que también introduce dos nuevas formas conocidas como “arresto digital” y el “secuestro cibernético”. El arresto digital representa un ciberdelito en auge en el que los perpetradores, a menudo haciéndose pasar por agentes del orden, engañan a las personas haciéndoles creer que su tarjeta SIM, tarjeta o cuenta bancarias está implicada en actividades delictivas. Aprovechando estas acusaciones inventadas, los delincuentes obligan a las víctimas a realizar pagos monetarios bajo presión, lo que las pone bajo arresto virtual hasta que se les entrega una compensación económica. De manera similar, el secuestro cibernético funciona como un esquema de extorsión mediante el cual se engaña a las víctimas para que crean que sus seres queridos están en peligro y se las obliga a pagar un rescate por su liberación (Sharkar y Shuka 2024, 9).

Además, el Departamento de Estado de Estados Unidos, explica como el control de víctimas se ha sofisticado con herramientas tecnológicas. Los tratantes utilizan aplicaciones de geolocalización⁵, que no necesariamente tienen que incorporar IA, para monitorear

⁵ Es conveniente precisar que no todas las tecnologías digitales utilizadas en el contexto de la TP implican el uso de IA. Herramientas como la geolocalización o el seguimiento de actividad en plataformas digitales pueden operar sin recurrir a sistemas de aprendizaje automático, basándose en funcionalidades técnicas predefinidas. En cambio, aplicaciones como el reconocimiento facial o el análisis conductual sí pueden incorporar técnicas de IA, particularmente algoritmos de *machine learning*, lo que permite automatizar decisiones a partir de grandes volúmenes de datos. Esta distinción es relevante en tanto que el valor añadido de la IA no reside en la mera digitalización de procesos, sino en su capacidad de automatización, predicción y escalabilidad.

movimientos, software espía en dispositivos personales y vigilancia constante a través de videollamadas. El TIP 2024 documenta casos donde explotadores mantienen control remoto sobre víctimas mediante amenazas de difundir material comprometedor capturado digitalmente (“sextorsión”), creando mecanismos de coacción que no requieren proximidad física (U.S. Department of State 2024). Otro impacto en el ámbito de la trata digital es referente a los métodos de pago digitales, particularmente criptomonedas, que han transformado las transacciones financieras vinculadas a la trata.

Con base en lo expuesto, el presente estudio tiene el objetivo de explicar cómo el desarrollo tecnológico y la inteligencia artificial (IA) han impactado tanto en el *modus operandi* de las redes de trata, sus formas de captación, como también su elusión de las persecuciones. En respuesta al anterior, se observa también el despliegue de contramedidas y el uso de las herramientas tecnológicas de IA en la lucha contra la trata. A estos efectos, el artículo se estructura en cinco sesiones. Esta primera que nos introduce al delito de la trata y el impacto provocado por las tecnologías. El segundo explica la evolución y el uso de las diferentes tecnologías digitales. El tercero que explica diferentes contramedidas adoptadas de lucha contra la trata digital. El cuarto que reflexiona sobre los dilemas éticos del uso de IA para enfrentar la TP. Y por último unas reflexiones finales sobre trata en el entorno digital.

La metodología de la investigación se enmarca en un enfoque cualitativo, basado en una revisión narrativa de la literatura, orientada a examinar de manera crítica el estado actual del conocimiento sobre la relación entre la TP y el desarrollo de tecnologías digitales, con especial atención al papel de la IA. A diferencia de las revisiones sistemáticas, este trabajo no persigue la exhaustividad ni la replicabilidad estricta del proceso de selección de fuentes, sino que adopta una estrategia de búsqueda flexible y orientada a la relevancia temática, con el objetivo de integrar aportaciones procedentes de distintos campos (derecho, criminología, estudios tecnológicos y políticas públicas).

La identificación de fuentes se llevó a cabo mediante consultas en bases de datos académicas de referencia, como Scopus, Web of Science y Google Scholar, así como a través de la revisión de informes institucionales elaborados por organismos internacionales (especialmente UNODC, OIM y el Departamento de Estado de Estados Unidos). Las búsquedas se realizaron utilizando combinaciones de palabras clave en inglés y español (entre ellas “human trafficking”, “trafficking in persons”, “artificial intelligence”, “digital technologies”, “online exploitation” o “machine learning”) empleadas de manera orientativa para localizar literatura relevante. No obstante, dichas palabras clave no se utilizaron

como parte de un protocolo sistemático cerrado, sino como herramientas de apoyo dentro de un proceso iterativo de exploración bibliográfica.

La selección de fuentes se basó en criterios de pertinencia y calidad académica, priorizando aquellos trabajos que abordan de forma directa la intersección entre TP y tecnologías digitales. Se incluyeron tanto artículos académicos como informes técnicos y documentos institucionales, con especial atención a contribuciones recientes (principalmente entre 2015 y 2024), sin excluir referencias anteriores consideradas fundamentales para la contextualización del fenómeno. El análisis de la información se realizó mediante una aproximación interpretativa de carácter cualitativo, orientada a identificar patrones recurrentes, tendencias emergentes, tensiones conceptuales y vacíos en la literatura existente. Este enfoque permite ofrecer una visión integrada del fenómeno, aunque no pretende establecer conclusiones generalizables en términos cuantitativos ni exhaustivos.

2. Las nuevas tecnologías y su relación con la trata

2.1. *Evolución del uso de Internet: La web 3.0 y la automatización del delito*

La TP ha evolucionado con los avances tecnológicos, transformando sus estrategias de captación, explotación y encubrimiento (Burbano y Hernández-Álvarez 2017). Internet ha permitido a los tratantes ampliar su alcance, optimizar métodos y diversificar mecanismos de explotación, marcando un punto de inflexión en la migración del delito del ámbito físico al virtual (Moldovan 2011). Desde la Web 1.0, con anuncios fraudulentos y correos electrónicos engañosos (Cotterill 2023), hasta la Web 2.0, con redes sociales y mensajería que facilitaron la manipulación psicológica y la creación de vínculos de confianza (Leng et al. 2014), la captación digital se ha sofisticado. Con la llegada de la Web 3.0, la IA, *blockchain*⁶ y el anonimato digital han añadido nuevos desafíos al dificultar la identificación de redes criminales y la localización de víctimas.

⁶ El *blockchain* es una tecnología de registro descentralizado que permite almacenar información de manera segura, transparente e inmutable. Su uso más conocido es en criptomonedas como *bitcoin*, pero también se ha aplicado en contratos inteligentes, trazabilidad de productos y verificación de identidades. En el contexto de la trata, ha sido utilizado tanto para el anonimato en transacciones ilícitas como para iniciativas de trazabilidad en la lucha contra la explotación.

La Web 3.0 ha marcado una nueva era en la digitalización de la TP, caracterizada por la automatización, la descentralización y el anonimato digital. A diferencia de las versiones anteriores de Internet, esta etapa incorpora IA, *blockchain* y aprendizaje automático, permitiendo a los tratantes operar con menor visibilidad y mayor eficiencia. La automatización mediante IA ha revolucionado la captación de víctimas, permitiendo a los tratantes utilizar algoritmos que identifican y contactan a personas vulnerables sin intervención humana directa (Kejriwal y Szekely 2022; Triplett 2024). Además, el anonimato digital, potenciado por el cifrado extremo a extremo y las VPN, ha dificultado el rastreo de las comunicaciones, facilitando el traslado de actividades delictivas a la *deep web*⁷ y aplicaciones descentralizadas (Graham 2023).

El uso de *blockchain* ha permitido ocultar flujos financieros ilícitos mediante criptomonedas, facilitando la financiación de redes de trata y la comercialización de contenido de explotación sexual sin dejar rastro (Portnoff et al. 2017, Rifki 2023). Asimismo, la generación de *deepfakes*⁸ ha incrementado la coacción digital, con videos manipulados utilizados para extorsionar a víctimas (Kupriianova y Kupriianova 2023). Una de las aplicaciones más preocupantes de la IA en el ámbito de la TP es la generación de contenido sintético, particularmente *deepfakes* con fines de explotación sexual (Aguilar 2025). El ICAT (2024) ha documentado casos donde los tratantes utilizan algoritmos de aprendizaje profundo para crear material pornográfico falso, pero extremadamente realista utilizando imágenes de víctimas reales. Esta tecnología permite a los explotadores multiplicar virtualmente a cada víctima, generando cientos de videos diferentes con una sola persona y maximizando ganancias mientras reducen la necesidad de reclutar nuevas víctimas. Adicionalmente, el

⁷ La *deep web* es la parte de Internet que no es accesible mediante motores de búsqueda convencionales como Google. Incluye bases de datos, correos, archivos protegidos por contraseñas y contenido de acceso restringido. A diferencia de la *dark web*, que requiere software especial para su acceso y es frecuentemente utilizada para actividades ilegales, la *deep web* comprende una amplia gama de información legítima, como documentos académicos, intranets corporativas y archivos gubernamentales no indexados.

⁸ Un *deepfake* es una técnica de IA que permite crear imágenes, videos o audios falsificados mediante el uso de aprendizaje profundo (*deep learning*). A través de redes neuronales generativas, los *deepfakes* pueden alterar rostros y voces en tiempo real, haciendo que una persona parezca decir o hacer algo que nunca ocurrió. Esta tecnología ha sido utilizada en la difusión de desinformación, manipulación política y pornografía no consensuada, convirtiéndose en una herramienta potencialmente peligrosa en la explotación y la TP.

material generado por IA puede ser personalizado según preferencias específicas de clientes, creando un producto “a medida” que aumenta su valor en mercados ilícitos.

Los sistemas conversacionales basados en IA, con uso de *chatbots* avanzados, están siendo implementados para automatizar el proceso de reclutamiento. La UNODC ha identificado operaciones donde estos sistemas mantienen simultáneamente conversaciones con docenas o cientos de potenciales víctimas, identificando vulnerabilidades mediante análisis lingüístico y adaptando estrategias persuasivas en tiempo real. Estos sistemas pueden operar 24/7, en múltiples idiomas y aplicando técnicas de manipulación psicológica refinadas mediante aprendizaje automático sobre interacciones previas exitosas. El resultado es un proceso de captación industrializado que amplifica exponencialmente el alcance de las redes de trata (UNODC 2024).

El control sobre las víctimas también ha evolucionado con la Web 3.0, implementando dispositivos de vigilancia con IA y geolocalización (véase supra) para asegurar su sometimiento continuo (Raets y Janssens 2018). Sistemas de reconocimiento facial y análisis comportamental⁹ monitorean constantemente a las personas explotadas, alertando a los tratantes sobre potenciales intentos de escape o comunicación con autoridades. La OIM ha documentado casos donde software de vigilancia mejorado con IA permite a un solo controlador supervisar efectivamente a docenas de víctimas simultáneamente, aumentando la eficiencia de las operaciones de explotación (OIM 2024). Todo esto permite la proliferación de lo que se ha denominado como “explotación híbrida”, donde las víctimas son explotadas tanto físicamente como digitalmente, maximizando los beneficios para los tratantes. Frente a estos desafíos, iniciativas como *Traffik Analysis Hub*¹⁰ han empleado *big data*¹¹ para mapear patrones de trata,

⁹ Las herramientas de análisis comportamental permiten examinar patrones de conducta a partir de datos generados por la actividad digital. En el contexto de la TP, estas técnicas pueden emplearse para anticipar comportamientos de las víctimas, identificar vulnerabilidades o detectar posibles intentos de fuga. Su eficacia depende de la disponibilidad y calidad de los datos, así como de la capacidad para interpretarlos adecuadamente, lo que introduce márgenes de incertidumbre en su aplicación.

¹⁰ Véase <https://www.traffikanalysis.org>

¹¹ El *big data* se refiere al procesamiento y análisis de grandes volúmenes de datos provenientes de múltiples fuentes. Su objetivo es identificar patrones, tendencias y correlaciones que no serían perceptibles mediante métodos tradicionales. En el contexto de la TP, el *big data* ha sido utilizado para detectar redes de explotación analizando interacciones en línea, transacciones financieras sospechosas y patrones de movilidad de las víctimas, mejorando la capacidad de prevención e intervención de las autoridades y organizaciones especializadas.

mientras que proyectos de identidad digital buscan ayudar a las víctimas a recuperar su estatus legal (Graham 2023).

2.2. *La importancia de la dark web y las plataformas digitales en las redes de trata*

El desarrollo de la *dark web* ha representado un desafío sin precedentes en la lucha contra la TP, proporcionando a las redes criminales un entorno en el que pueden operar con un alto grado de anonimato y con menor riesgo de ser detectadas por las autoridades (Burbano y Hernández-Álvarez 2017). A diferencia de lo que se conoce como “superficie de Internet”, donde la mayoría de las interacciones ocurren en plataformas indexadas por motores de búsqueda convencionales, la *dark web* constituye un espacio en el que la actividad es intencionadamente opaca, ya que solo es accesible mediante software especializado, como el navegador Tor (*The Onion Router*), que encripta las conexiones y permite la navegación anónima (Sarkar 2024). Esta característica ha convertido a la *dark web* en un refugio para actividades ilícitas, entre ellas, el comercio de personas con fines de explotación sexual, laboral e incluso el tráfico de órganos.

Podemos decir que la relación entre la TP y la *dark web* se basa en tres elementos fundamentales: el anonimato, la descentralización y la facilidad para realizar transacciones financieras sin dejar rastro. En primer lugar, el anonimato digital garantiza que los tratantes puedan interactuar con compradores y otros intermediarios sin revelar su identidad ni su ubicación. Mientras que en la Web 2.0 las redes sociales y las plataformas de mensajería ya ofrecían cierto nivel de discreción, la *dark web* lleva esta protección al extremo, utilizando redes cifradas que imposibilitan el rastreo de los datos de los usuarios (Graham 2023). Este factor ha sido clave para la consolidación de mercados clandestinos donde se comercializan víctimas de trata, publicitadas a través de descripciones detalladas y, en muchos casos, con material fotográfico que prueba su disponibilidad para la explotación (Sarkar 2024).

La descentralización es otro aspecto crucial en el funcionamiento de la *dark web* como canal para la TP. A diferencia de la Internet convencional, donde los servidores están alojados en infraestructuras controladas por empresas y gobiernos que pueden eliminar contenido ilegal bajo requerimientos legales, la *dark web* opera a través de una red distribuida en la que los servidores están ubicados en múltiples países, lo que hace extremadamente difícil su intervención (Shivani 2024). Esta arquitectura permite que las redes de trata trasladen sus operaciones de

un servidor a otro con rapidez, evitando la detección y el cierre de sus plataformas. Además, la falta de regulación y cooperación internacional en torno a estos sitios ha permitido que los sitios dedicados a la explotación persistan durante largos períodos sin ser desmantelados.

En términos financieros, la *dark web* ha facilitado el crecimiento de la trata mediante el uso de criptomonedas como *bitcoin* y *monero*, que ofrecen un alto nivel de anonimato en las transacciones. Estas monedas digitales permiten que los tratantes reciban pagos sin necesidad de utilizar el sistema bancario tradicional, lo que dificulta el rastreo del dinero y la identificación de los involucrados (Naheem 2020). Investigaciones sobre cibercriminalidad han demostrado que en foros clandestinos se realizan transacciones de alto valor por víctimas destinadas a la explotación sexual o laboral, así como por servicios de producción de material de abuso sexual infantil, una de las formas más lucrativas de explotación en el ciberespacio (Naheem 2020; Portnoff et al. 2017).

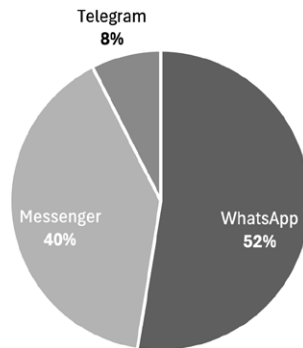
Por otro lado, las redes sociales han sido uno de los principales canales utilizados para la captación de víctimas en el entorno digital. Plataformas como Facebook, Instagram, TikTok y Twitter han proporcionado a los tratantes un espacio idóneo para identificar, contactar y manipular a personas vulnerables (Rentzsch 2021). El uso de algoritmos y análisis de datos en redes sociales han potenciado la capacidad de los tratantes para seleccionar a sus víctimas con mayor precisión (Moser 2021). Las plataformas digitales recopilan información detallada sobre sus usuarios, incluyendo sus interacciones, intereses, ubicaciones y redes de contactos (Latoner 2011). Esta disponibilidad de datos ha sido aprovechada por las redes de trata para identificar perfiles vulnerables, como adolescentes con problemas familiares, mujeres en situación de precariedad económica o migrantes en búsqueda de oportunidades laborales. En algunos casos, los tratantes utilizan anuncios dirigidos o interacciones específicas para atraer a sus víctimas, adaptando sus mensajes a las necesidades y expectativas de cada objetivo (Moser 2021).

Además de las redes sociales, las aplicaciones de mensajería instantánea han desempeñado un papel fundamental en la captación y control de las víctimas. Plataformas como WhatsApp, Telegram, Signal y Messenger han permitido a los tratantes establecer comunicaciones privadas con sus objetivos, evitando la supervisión de terceros y reduciendo la posibilidad de ser detectados (Polaris 2018). La facilidad para compartir imágenes, videos y enlaces a sitios externos ha facilitado la manipulación de las víctimas, quienes muchas veces son persuadidas a enviar información personal o a participar en actividades que luego son utilizadas como herramientas de chantaje y coerción (Geldenhuis 2019). La encriptación de extremo a extremo en muchas

de estas aplicaciones ha dificultado la intervención de las autoridades, permitiendo que las redes de trata operen con un alto nivel de discreción y anonimato (Sarkar 2024).

Figura 1

Aplicaciones de mensajería más usadas para la captación de la trata de seres humanos



Fuente: Elaboración propia con base en Rentzsch (2021), UNODC (2020) y OSCE (2020).

Uno de los fenómenos más alarmantes en el uso de plataformas digitales para la captación es la explotación de sitios de citas y aplicaciones de “*sugardating*”. Plataformas como Tinder, Badoo, Grindr y Seeking han sido utilizadas por los tratantes para atraer víctimas con promesas de relaciones sentimentales o acuerdos financieros que, en realidad, conducen a situaciones de explotación sexual y laboral (Geldenhuys 2019). En muchos casos, los tratantes se presentan como benefactores o parejas potenciales, estableciendo una relación de confianza antes de introducir gradualmente elementos de control y coerción. La falta de regulaciones estrictas en estas aplicaciones ha permitido que los tratantes operen con facilidad, utilizando perfiles falsos y cambiando constantemente de identidad para evadir la detección.

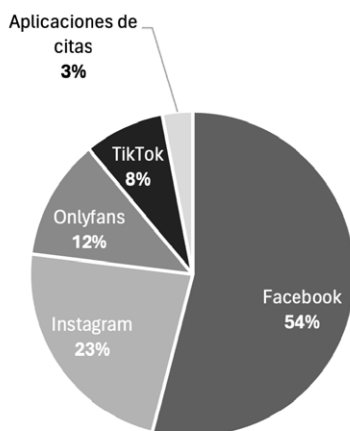
Los sitios web de anuncios clasificados también han sido un medio recurrente para la captación de víctimas. Páginas como Craigslist, Backpage (antes de ser cerrada por las autoridades) y Locanto han sido utilizadas por redes de trata para publicar ofertas de trabajo fraudulentas que atraen a personas en busca de empleo (DeLateur 2016, Portnoff et al. 2017). Muchas de estas ofertas prometen salarios elevados,

condiciones de trabajo atractivas y oportunidades en el extranjero, pero en realidad conducen a situaciones de explotación en las que las víctimas pierden su autonomía y son sometidas a condiciones abusivas (Portnoff et al. 2017). En algunos casos, los tratantes utilizan estos sitios para anunciar directamente servicios de explotación sexual, camuflados bajo términos ambiguos que dificultan su identificación por parte de las plataformas y los organismos de control (DeLateaur 2016).

El auge de plataformas de transmisión en vivo y contenido por suscripción también ha sido explotado por las redes de trata para la explotación de sus víctimas. Sitios como *OnlyFans*, *Chaturbate* y sitios similares han facilitado nuevas formas de explotación sexual en las que las víctimas son obligadas a realizar actos frente a una cámara para audiencias anónimas en todo el mundo (Rifki 2023). A diferencia de la trata tradicional, en la que la explotación ocurría en un espacio físico determinado, estas plataformas han permitido que la explotación se lleve a cabo de manera remota, dificultando aún más la identificación y el rescate de las víctimas. En muchos casos, los tratantes ejercen control sobre las víctimas mediante amenazas, chantaje o manipulación emocional, asegurando su obediencia sin necesidad de contacto físico (Marion y Hufgard 2025).

Figura 2

Las plataformas de redes sociales más usadas en la captación de la trata de seres humanos



Fuente: Elaboración propia con base en Rentzsch (2021), UNODC (2020), OSCE (2020).

2.3. *El uso de la IA en el control y explotación de las víctimas*

El desarrollo de la IA ha generado transformaciones profundas en múltiples ámbitos, desde la automatización de procesos hasta la optimización de estrategias comerciales y de comunicación. Sin embargo, al igual que ocurre con muchas innovaciones tecnológicas, la IA también ha sido aprovechada por redes criminales para sofisticar sus métodos de operación (King et al. 2020). En el contexto de la trata de seres humanos, la IA no solo ha sido utilizada para la captación de víctimas, sino también para su control y explotación, permitiendo a los tratantes reducir los riesgos de detección y maximizar sus ganancias con menor exposición personal (Jeong 2020). La implementación de sistemas de monitoreo, algoritmos de manipulación psicológica, herramientas de vigilancia digital y automatización de la explotación han convertido a la IA en una aliada estratégica para quienes se benefician de la trata, generando nuevos desafíos en la lucha contra este delito.

El control de las víctimas mediante IA se ha desarrollado en distintos niveles, abarcando desde la vigilancia constante hasta la manipulación de su entorno digital. Uno de los mecanismos más utilizados es el monitoreo en tiempo real a través de dispositivos conectados, como cámaras de seguridad y sensores de movimiento (Raets y Janssens 2018). En muchos casos, las víctimas de trata son obligadas a portar teléfonos móviles con aplicaciones de rastreo que permiten a sus explotadores conocer su ubicación exacta en todo momento. Este tipo de tecnología impide que las víctimas escapen o pidan ayuda, ya que cualquier intento de abandonar el perímetro controlado puede ser detectado de inmediato (Raets y Janssens 2018). La IA también ha sido integrada en sistemas de reconocimiento facial y análisis de comportamiento, utilizados por los tratantes para vigilar a las víctimas en espacios de explotación como burdeles, fábricas clandestinas o centros de mendicidad forzada. Estos sistemas permiten detectar cualquier intento de resistencia, facilitando la intervención de los explotadores antes de que la víctima pueda escapar o contactar con el exterior (Ijiga et al. 2024).

Otro aspecto clave en el uso de la IA para el control de las víctimas es la manipulación psicológica a través de herramientas digitales avanzadas. La IA ha sido utilizada para generar contenido persuasivo diseñado específicamente para mantener a las víctimas bajo el dominio de sus explotadores (Hong 2023). Los *chatbots* programados con IA pueden simular conversaciones humanas, que extrapolándolo al contexto de la trata podría enviar mensajes constantes a las víctimas

para reforzar su dependencia emocional y evitar que busquen ayuda (Balcombe 2023). En algunos casos, los tratantes han utilizado IA para manipular imágenes y videos, creando material falso con el que amenazan a las víctimas con su divulgación si intentan huir o denunciar su situación (Sarkar 2024). Estas estrategias de coerción digital han demostrado ser altamente efectivas, ya que generan un clima de miedo y desesperanza que limita las posibilidades de resistencia.

La explotación de las víctimas también ha sido transformada por la IA, particularmente en el ámbito de la explotación sexual en línea. Plataformas de transmisión en vivo y contenido por suscripción han integrado herramientas de IA que permiten a los tratantes gestionar múltiples víctimas al mismo tiempo, optimizando sus ganancias y reduciendo la necesidad de supervisión directa (Demetis y Kietzmann 2021). La IA puede ser utilizada para analizar las preferencias de los consumidores de contenido sexual, adaptando las interacciones de las víctimas en función de la demanda del mercado. En algunos casos, los tratantes han desarrollado algoritmos capaces de gestionar automáticamente las sesiones de explotación, programando respuestas predeterminadas y ajustando las transmisiones en función de la interacción del público (Hickle 2017). Este nivel de automatización ha permitido que la explotación digital alcance una escala sin precedentes, eliminando muchas de las limitaciones que anteriormente restringían la rentabilidad del delito.

Otro fenómeno preocupante es el uso de *deepfake* y generación de contenido sintético en la TP. La IA ha permitido la creación de videos y fotografías hiperrealistas en los que las víctimas aparecen participando en actos sexuales sin su consentimiento (Sharma et al. 2023). Este material, producido sin necesidad de la presencia física de la víctima, es utilizado para extorsionarlas o para comercializarlo en mercados clandestinos de la *dark web* (Hong 2023). En algunos casos, los tratantes han utilizado IA para crear perfiles falsos en plataformas de contenido para adultos, simulando la existencia de una víctima y generando ingresos sin necesidad de interacción humana real. Esta tendencia ha abierto un nuevo frente en la explotación digital, en el que la IA no solo facilita la TP, sino que también genera nuevas formas de victimización que son aún más difíciles de rastrear y combatir (Nour y Gelfand 2022).

Además de la explotación sexual, la tecnología ha sido utilizada para el control y explotación laboral de las víctimas de trata (Beate y Geneva 2012; LeBaron y Crane 2018). En fábricas ilegales y centros de trabajo forzado, los tratantes han implementado sistemas de IA para optimizar la producción y supervisar a los trabajadores en condiciones

de esclavitud moderna. Cámaras con análisis de movimiento detectan si un trabajador reduce su ritmo o intenta abandonar el área de trabajo, activando alertas automáticas que informan a los explotadores (Athreya 2020). Estas herramientas han consolidado un modelo de vigilancia digital que reduce la necesidad de supervisión física, permitiendo a los tratantes controlar a un mayor número de víctimas con menores costos operativos.

3. Herramientas tecnológicas en la lucha contra la trata digital

El desarrollo de plataformas basadas en IA ha transformado la lucha contra la TP, facilitando la detección temprana de redes de explotación. A diferencia de los métodos tradicionales, que dependen de denuncias o intervenciones policiales, estas herramientas automatizan el monitoreo de actividades delictivas y optimizan estrategias de respuesta (Dutta 2020). La digitalización de la trata ha generado un gran volumen de datos dispersos en redes sociales, foros de la *dark web* y registros financieros (Graham 2023, Rentzsch 2021, Sarkar 2024). La IA permite filtrar y correlacionar esta información en tiempo real, identificando patrones sospechosos y localizando víctimas (Dutta 2020, Orantes 2018). Algoritmos avanzados analizan anuncios de explotación, transacciones irregulares y perfiles en redes sociales vinculados a la captación de víctimas (Orantes 2018).

3.1. *Traffik Analysis Hub: mapeo de redes de trata*

El *Traffik Analysis Hub* (TAHub) es una de las iniciativas más avanzadas en la aplicación de IA y análisis de datos para la detección y desmantelamiento de redes de trata. Desarrollado por IBM en colaboración con la organización Stop The Traffik y otros actores gubernamentales y del sector privado, su principal objetivo es proporcionar una visión global en tiempo real de los patrones de trata, permitiendo una respuesta más eficiente y coordinada (Khanal 2020; TAHub s.f.).

El TAHub recopila y analiza grandes volúmenes de datos provenientes de diversas fuentes, incluyendo informes de ONG, registros policiales, denuncias de víctimas y transacciones financieras sospechosas (Khanal 2020). Mediante algoritmos avanzados, identifica tendencias ocultas, correlaciona casos aparentemente aislados y genera alertas sobre posibles redes de explotación (Perussi y Correa 2024).

Uno de sus principales logros es superar la fragmentación de datos entre organismos, un problema que históricamente ha dificultado la lucha contra la trata (Perussi y Correa 2024). A través de un mapa global de trata, la plataforma permite visualizar en tiempo real las rutas utilizadas por las redes criminales, los métodos de captación y los focos de explotación (TAHub s.f.). Además, el aprendizaje automático permite generar modelos predictivos que alertan sobre zonas de alto riesgo y posibles patrones de trata antes de que ocurran los delitos.

Uno de los aspectos más innovadores del TAHub es su capacidad para detectar conexiones ocultas, tal y como estos autores infieren indirectamente del análisis de Perussi y Correa (2024). La trata opera en la clandestinidad, lo que dificulta su detección por métodos tradicionales. Sin embargo, al analizar miles de registros y correlacionar variables como ubicaciones, transacciones y anuncios en línea, la plataforma ha permitido identificar redes de explotación previamente invisibles para las autoridades (Perussi y Correa 2024). En términos de prevención, el TAHub también ha sido utilizado para diseñar campañas de sensibilización dirigidas a grupos en riesgo, basándose en datos sobre las tácticas de captación más frecuentes en diferentes regiones. Esto representa avances relevantes en la agregación de datos sobre TP, aunque su impacto depende en gran medida del nivel de cooperación estatal y de la calidad de los datos aportados, por lo que no eliminar completamente los problemas de fragmentación existentes.

3.2. *PhotoDNA: Identificación de material de explotación*

La tecnología de análisis de imágenes ha sido clave en la lucha contra la explotación infantil en entornos digitales. *PhotoDNA*, desarrollado por Microsoft junto con el NCMEC, se ha convertido en una herramienta esencial desde su implementación en 2009 (Microsoft s.f., Singh 2020). Adoptado por grandes plataformas tecnológicas y fuerzas de seguridad, ha facilitado la detección y eliminación de contenido ilegal, contribuyendo al desmantelamiento de redes de trata (Steinebach 2023). *PhotoDNA* utiliza “*hashing* perceptual” para generar identificadores únicos de imágenes, permitiendo reconocer contenido ilegal incluso si ha sido editado (Singh 2020, Steinebach 2024). Su integración en plataformas como Facebook, Twitter y Google ha permitido eliminar millones de imágenes ilegales, evitando su redistribución (Microsoft s.f.). Además, ha sido empleado por Interpol y el FBI en la identificación de víctimas y agresores (Steinebach 2023).

Su capacidad para procesar grandes volúmenes de datos en tiempo real es crucial en la lucha contra la trata digital, donde el contenido ilegal suele publicarse y eliminarse rápidamente (Sarkar 2024). También ha facilitado la recopilación de pruebas para procesos judiciales, fortaleciendo casos contra redes criminales (Microsoft s.f.; Singh 2020). Sin embargo, su implementación ha generado debates sobre privacidad y regulación, con preocupaciones sobre la vigilancia digital y posibles falsos positivos (Steinebach 2024). Aunque Microsoft ha establecido protocolos estrictos, *PhotoDNA* solo detecta imágenes ya registradas, lo que obliga a desarrollar tecnologías complementarias para identificar contenido inédito (Singh 2020, Steinebach 2024).

3.3. *Traffic Jam: Análisis de datos forenses*

El análisis forense de datos es fundamental en la lucha contra la TP, facilitando la identificación de víctimas y la desarticulación de redes criminales. *Traffic Jam*, desarrollada por Marinus Analytics, emplea IA para analizar grandes volúmenes de información y acelerar la detección de casos en plataformas digitales (Graham 2023; Spice 2019). Su uso por parte de agencias como el FBI y el Departamento de Seguridad Nacional ha optimizado las investigaciones de trata y explotación infantil (Amazon 2020).

Traffic Jam examina anuncios en línea relacionados con la explotación sexual mediante técnicas de procesamiento de lenguaje natural y reconocimiento de imágenes (Marinus Analytics s.f.). Identifica patrones entre publicaciones, permitiendo conectar perfiles aparentemente aislados y mapear redes de trata (Pittsburgh Technology Council s.f.). Su función de reconocimiento facial ha sido clave en la identificación de víctimas al comparar imágenes extraídas de anuncios con bases de datos de personas desaparecidas, incluso si han sido alteradas (Amazon 2020).

Además de identificar víctimas, la plataforma permite rastrear redes delictivas analizando anuncios, contactos y movimientos financieros sospechosos, incluyendo transacciones en criptomonedas asociadas con la explotación sexual (Marinus Analytics s.f.). Esta capacidad ha sido esencial para dismantelar organizaciones criminales transnacionales. A medida que las redes criminales adoptan nuevas tácticas, como *deepfakes* y cifrado extremo, *Traffic Jam* ha debido evolucionar para seguir detectando patrones delictivos (Spice 2019). Sin embargo, su uso también plantea desafíos en materia de

privacidad, ya que el análisis masivo de datos requiere regulaciones adecuadas para evitar abusos (Pittsburgh Technology Council s.f.).

3.4. *Spotlight y TraffickCam: Inteligencia artificial en la identificación de ubicaciones y víctimas*

El uso de IA ha permitido el desarrollo de herramientas como *Spotlight* y *TraffickCam*, que optimizan la identificación de víctimas y la localización de lugares de explotación. Aunque con enfoques distintos, ambas plataformas emplean análisis de datos avanzados para acelerar la detección y mejorar la capacidad de respuesta en casos de trata (Spotlight s.f.; TraffickCam s.f.).

Spotlight, desarrollada por Thorn, analiza grandes volúmenes de datos de anuncios en línea y redes sociales para detectar patrones de trata y correlacionar casos con víctimas reportadas (Runyon 2025). Su IA permite priorizar casos según el nivel de riesgo, facilitando la asignación eficiente de recursos (Spotlight s.f.). Desde su lanzamiento, ha identificado más de 24.000 víctimas y apoyado más de 17.000 investigaciones (Spotlight s.f.), reduciendo el tiempo de análisis de semanas a segundos.

Por otro lado, *TraffickCam*, creada por el Exchange Initiative, se centra en la identificación de ubicaciones de explotación. Su base de datos contiene millones de imágenes de habitaciones de hotel enviadas por ciudadanos y fuerzas de seguridad, permitiendo a los investigadores comparar fotos de víctimas con su archivo y localizar el lugar exacto donde fueron fotografiadas (Stylianou et al. 2017). Su sistema de visión artificial analiza detalles como muebles y cortinas para detectar coincidencias, facilitando rescates rápidos (TraffickCam s.f.).

A pesar de su impacto, ambas herramientas enfrentan desafíos. *Spotlight* debe adaptarse al uso de encriptación y plataformas descentralizadas por parte de los tratantes, mientras que *TraffickCam* depende de la actualización constante de su base de datos y la cooperación del público y la industria hotelera. También persisten debates sobre el equilibrio entre vigilancia y privacidad en su implementación (Stylianou et al. 2019). Incluso con sus deficiencias, *Spotlight* y *TraffickCam* representan avances significativos en el uso de IA para la lucha contra la TP, abordando el problema desde distintas perspectivas, pero con un impacto complementario.

4. Limitaciones legales y cooperación internacional en el desarrollo de tecnología contra la trata de personas

Antes de proceder con el análisis de las limitaciones identificadas, estos autores tras el análisis de las herramientas expuestas proponen una categorización original que permite entender la tecnología no solo como un recurso, sino como un ecosistema de fuerzas contrapuestas. Se propone clasificar el impacto de la IA en tres dimensiones de respuestas que son resumidas en la tabla1.

Tabla 1
Taxonomía funcional de la IA en la TP

Dimensión	Objetivo principal	Definición
Dimensión de detección reactiva	Identificación	Herramientas como <i>PhotoDNA</i> y <i>Spotlight</i> que operan sobre el daño ya causado, buscando material existente o víctimas activas.
Dimensión de inteligencia predictiva	Prevención	El uso de <i>Big Data</i> en <i>TAHub</i> para mapear flujos antes de que se consoliden las rutas.
Dimensión forense-operativa	Desarticulación	Sistemas como <i>Traffic Jam</i> que, mediante el procesamiento de lenguaje natural, permiten dismantelar la estructura del negocio tras la pantalla.

Fuente: Elaboración propia.

Esta clasificación permite concluir que la lucha contra la trata digital no fracasa por falta de tecnología, sino por la falta de interoperabilidad entre estas tres dimensiones, un vacío que los tratantes aprovechan mediante la descentralización de la Web 3.0. Mientras que las redes de trata han sabido adaptarse con rapidez a los avances digitales, los marcos normativos y las infraestructuras tecnológicas han demostrado ser insuficientes para abordar la complejidad del fenómeno, generando un desfase entre el desarrollo de nuevas herramientas y su regulación adecuada (Deeb-Swihart et al. 2022). La ausencia de una legislación armonizada a nivel global, la opacidad de los algoritmos y las deficiencias en la cooperación internacional constituyen algunos de los

principales desafíos que deben resolverse para maximizar el impacto de la IA en la lucha contra este delito (Mehra y Sharif 2024).

Uno de los problemas más graves en este contexto es la fragmentación legal en torno al uso de IA para la detección de la TP. En la actualidad, no existe un marco normativo universal que establezca criterios claros sobre la implementación y los límites de estas tecnologías, lo que genera vacíos legales que pueden ser explotados tanto por redes criminales como por actores gubernamentales o privados con intereses particulares (Mehra y Sharif 2024). Con la aprobación del Reglamento de Inteligencia Artificial de la UE (AI Act), Europa se ha convertido en la primera gran jurisdicción en adoptar un enfoque integral para regular el desarrollo y uso de la IA, estableciendo un sistema de clasificación de riesgos y requisitos específicos para las aplicaciones de alto impacto en la sociedad (Gstrein et al. 2024).

El *AI Act* establece cuatro niveles de riesgo para las aplicaciones de IA, diferenciando entre aquellas que presentan un riesgo inaceptable, alto, limitado o mínimo (Laux et al. 2024). Las tecnologías consideradas de alto riesgo incluyen sistemas de IA utilizados en el ámbito de la seguridad y la aplicación de la ley, lo que afecta directamente a herramientas de detección de trata como el reconocimiento facial, la predicción delictiva basada en algoritmos y el análisis automatizado de datos en redes sociales y plataformas digitales (Gstrein et al. 2024).

Uno de los aspectos más controvertidos del *AI Act* es la restricción del uso de tecnologías de reconocimiento facial en espacios públicos, lo que impacta directamente en los esfuerzos para localizar y rescatar víctimas de trata en aeropuertos, estaciones de transporte y otras zonas de alta vulnerabilidad (European Parliament 2021). Aunque la normativa permite excepciones para la lucha contra el crimen organizado, estas aplicaciones están sujetas a autorizaciones judiciales previas y controles estrictos, lo que puede ralentizar investigaciones en situaciones donde el tiempo es un factor determinante. A pesar de su efectividad en la identificación de personas desaparecidas y víctimas de trata, el uso excesivo del reconocimiento facial también ha suscitado preocupaciones sobre privacidad y vigilancia masiva (Girasa 2020).

En el ámbito de la cooperación internacional, las diferencias en la regulación tecnológica han generado obstáculos en el intercambio de información y la persecución de delitos transnacionales (Mehra y Sharif 2024). La TP es un crimen global, pero los sistemas de IA utilizados en su combate suelen estar restringidos por legislaciones nacionales que limitan la interoperabilidad de bases de datos y la colaboración entre agencias. En algunos países, las regulaciones sobre privacidad impiden compartir datos sobre víctimas con otras jurisdicciones, lo que dificulta

la identificación de redes de trata que operan a través de múltiples fronteras (Mehra y Sharif 2024).

A pesar de estas limitaciones, la cooperación internacional ha sido clave en el desarrollo de nuevas tecnologías para la lucha contra la TP. Organismos como Naciones Unidas y la Unión Europea han promovido la creación de estándares globales para el uso de IA en la lucha contra la trata (Deeb-Swihart et al. 2022). La UNODC (2024) ha desarrollado marcos normativos orientados a la cooperación entre países en la investigación de delitos de explotación en línea, destacando la necesidad de regular el uso del reconocimiento facial, el análisis de datos masivos y la vigilancia digital dentro de un marco de respeto a los derechos humanos (Annouz s.f., Acosta 2024). Sin embargo, la implementación de estos estándares varía según la región, lo que ha generado brechas en la efectividad de las herramientas tecnológicas en función de las capacidades legales y técnicas de cada país (Annouz s.f.).

Otro de los avances recientes en cooperación internacional ha sido la implementación de sistemas de rastreo financiero y criptográfico en la detección de transacciones relacionadas con la TP (Popov y Masolletti 2021). Dado que muchas redes criminales han migrado hacia el uso de criptomonedas para evadir los sistemas bancarios tradicionales, organismos como Interpol, Europol y el Grupo de Acción Financiera Internacional (GAFI) han desarrollado algoritmos basados en IA para identificar flujos de dinero sospechosos (Susanti y Prastyanti 2024, Ríos 2025). Sin embargo, la efectividad de estos sistemas se ve limitada por la falta de una regulación uniforme sobre criptomonedas en el ámbito internacional, lo que permite que las redes de trata sigan operando en países con regulaciones más laxas.

Otro problema es la asimetría tecnológica entre países, que impide que todas las regiones puedan beneficiarse de los avances en IA de la misma manera. Mientras que en América del Norte y Europa se han desarrollado herramientas sofisticadas de detección y rastreo, muchas naciones en desarrollo carecen de la infraestructura técnica y los recursos humanos necesarios para implementar estas soluciones (Ijiga, Aboi et al. 2024). Esto genera una brecha en la capacidad de respuesta frente a la trata, permitiendo que las redes criminales trasladen sus operaciones a regiones con menor vigilancia tecnológica.

Consideraciones finales

Las transformaciones analizadas permiten sostener que el desarrollo de tecnologías digitales y, en particular, de la IA, no solo ha

intensificado la TP, sino que ha reconfigurado sus dinámicas operativas. En este sentido, la trata en entornos digitales ya no puede entenderse únicamente como una extensión del delito tradicional, sino como un fenómeno que incorpora nuevas lógicas de funcionamiento, caracterizadas por la automatización de procesos, la ampliación del alcance de las redes criminales y la eliminación de los cuellos de botella humanos que tradicionalmente limitaban la escala de la captación y explotación, permitiendo una gestión masiva de víctimas con una infraestructura mínima. Este cambio contribuye a explicar tanto la creciente complejidad del fenómeno como las limitaciones de los enfoques convencionales de análisis e intervención.

La principal aportación de este trabajo consiste en la identificación de una tipología funcional de los usos de la IA en las distintas fases de la TP: captación, control, explotación y ocultación. Esta propuesta permite articular una lectura más precisa del fenómeno, al mostrar cómo la tecnología no opera de manera homogénea, sino que incide de forma diferenciada en cada una de estas fases. De este modo, se supera una aproximación meramente descriptiva o tecnológica, ofreciendo un marco analítico que facilita la comprensión de los mecanismos específicos a través de los cuales la IA contribuye a la reproducción y sofisticación de la TP.

A partir de esta tipología, se pone de relieve que el impacto de la IA no es uniforme. Los usos vinculados a la captación y la explotación inciden de manera más directa en la generación y mantenimiento de situaciones de victimización, al facilitar tanto la identificación de personas vulnerables como la maximización de los beneficios derivados de su explotación. Por su parte, los usos asociados al control y la ocultación refuerzan la sostenibilidad de las redes de trata, dificultando su detección y aumentando su capacidad de adaptación. Esta diferenciación tiene implicaciones relevantes desde el punto de vista jurídico, en la medida en que evidencia la necesidad de respuestas regulatorias ajustadas a la función específica que desempeña la tecnología en cada fase del delito.

En este contexto, el análisis pone de manifiesto una tensión estructural entre el uso de herramientas basadas en IA para la detección y persecución de la TP y la necesidad de garantizar derechos fundamentales como la privacidad o la protección de datos. Esta tensión no puede resolverse mediante soluciones simplificadoras. Por el contrario, exige el desarrollo de marcos de gobernanza que permitan integrar el uso de estas tecnologías en la lucha contra la TP sin comprometer las garantías jurídicas. Ello implica avanzar hacia modelos de regulación que combinen supervisión efectiva, criterios de proporcionalidad y mecanismos de

rendición de cuentas. Bajo esta lógica, se concluye que la eficacia técnica no debe desplazar a una supervisión humana significativa: los sistemas de IA deben operar como soportes analíticos de alerta temprana y nunca como mecanismos de prueba automatizada que eludan el escrutinio judicial o los derechos de defensa.

Desde esta perspectiva, la respuesta a la TP en el entorno digital requiere una articulación más coherente entre innovación tecnológica, regulación jurídica y cooperación internacional. En particular, resulta necesario incorporar de forma más explícita la dimensión tecnológica en los marcos normativos existentes, al tiempo que se refuerzan las capacidades institucionales para el uso estratégico de herramientas basadas en IA¹². Asimismo, la naturaleza transnacional del fenómeno hace imprescindible avanzar en mecanismos de cooperación que permitan superar la fragmentación actual en el acceso y uso de datos relevantes para la detección de redes de trata. El éxito de la respuesta institucional no dependerá únicamente de la potencia de cálculo de los algoritmos, sino de la creación de marcos de interoperabilidad de datos que permitan una respuesta global tan interconectada como la propia arquitectura del delito.

En definitiva, la TP en el entorno digital plantea desafíos que no pueden abordarse únicamente desde categorías tradicionales. La IA, en tanto que elemento que atraviesa y reconfigura las distintas fases del delito, obliga a adoptar enfoques analíticos y regulatorios más precisos, diferenciados y orientados al riesgo. Solo a través de esta aproximación será posible desarrollar respuestas que resulten efectivas frente a la evolución del fenómeno sin comprometer la protección de los derechos fundamentales.

Referencias

- Acosta, Alejandro. 2024. «The crime of human trafficking and the use of technology for the protection of human rights. Reference to the Dominican case». *Revista Científica Panorámica de los DDHHyDIH* 2(2): 21-39.
- Aguilar, Oswaldo. 2025. «Inteligencia artificial para la detección y prevención de la trata de personas». *Revista Mexicana de Ciencias Penales* 8(26): 3-26. Doi: 10.57042/rmcp.v9i26.895.

¹² Existe una tensión estructural entre la necesidad de rapidez en la investigación de la trata digital y las garantías jurídicas, como la exigencia de autorización judicial para determinadas medidas de vigilancia. Lejos de ser contradictorias, ambas dimensiones deben entenderse como complementarias. En este sentido, el reto no es reducir garantías, sino diseñar marcos normativos que permitan respuestas ágiles sin comprometer los derechos fundamentales.

- Amazon. 2020. *Marinus analytics case study*. Acceso el 28 de febrero de 2025: <https://aws.amazon.com/solutions/case-studies/marinus-analytics-databases-case-study/>.
- Annouz, Meryam. s.f. *Opinion piece: transnational cooperation and artificial intelligence based anti-corruption tools*. United Nations: Office on Drugs and Crime. Acceso el 25 de febrero de 2025: https://www.unodc.org/corruption/en/news/2024-09-25_opinion-piece_transnational-cooperation-and-artificial-intelligence-based-anti-corruption-tools-ai-acts.html.
- Athreya, Bama. 2020. «Slaves to technology: worker control in the surveillance economy». *Anti-Trafficking Review* 15: 82-101. Doi: 10.14197/atr.201220155.
- Balcombe, Luke. 2023. «AI chatbots in digital mental health». *Informatics* 10(4): 82. Doi: 10.3390/informatics10040082.
- Beate, Andrees y Patrick Geneva. 2012. «Forced labor: coercion and exploitation in the private economy». *Contemporary Sociology* 41(1): 117-117. Doi: 10.1177/0094306111430634.
- Burbano, Danilo y Myriam Hernández-Álvarez. 2017. «Identifying human trafficking patterns online». *2017 IEEE Second Ecuador Technical Chapters Meeting*, octubre, 1-6. Doi: 10.1109/ETCM.2017.8247461.
- Correa da Silva, Waldimeiry. 2018. *Regime internacional de enfrentamento ao tráfico de pessoas: avanços e desafios para a proteção dos direitos humanos*. Río de Janeiro: Lumen Juris.
- Cotterill, Diane. 2023. «The impact of social media, the Internet, and legislation on online minor sex trafficking». *Journal of Digital Life and Learning* 3(2): 2. Doi: 10.51357/jdll.v3i2.226.
- Deeb-Swihart, Julia, Alex Endert y Amy Bruckman. 2022. «Ethical tensions in applications of AI for addressing human trafficking: A human rights perspective». *Proc. ACM Hum.-Comput. Interact.* 6: 295: 1-29. Doi: 10.1145/3555186.
- DeLateaur, Monica. 2016. «From craigslist to backpage.com conspiracy as a strategy to prosecute third-party websites for sex trafficking». *Santa Clara Law Review* 56: 531-592.
- Demetis, Dionysios y Jan Kietzmann. 2021. «Online child sexual exploitation: a new MIS challenge». *Journal of the Association for Information Systems* 22(1): 5-40. Doi: 10.17705/1jais.00652.
- Dutta, Mondira. 2020. «Role of technology in combatting human trafficking». *Bulletin of the Karaganda University History* 100(4): 57-64. Doi: 10.31489/2020hph4/57-64.
- European Parliament. 2021. *Regulating facial recognition in the EU: In depth analysis*. Acceso el 27 de febrero de 2025: <https://data.europa.eu/doi/10.2861/140928>.
- Geldenhuys, Kotie. 2019. «The role of social media in facilitating human trafficking». *Servamus Community-based Safety and Security Magazine* 112(7): 18-20. Doi: 10.10520/EJC-16b23bbdaa.
- Girasa, Rosario. 2020. «Ethics and privacy I: facial recognition and robotics». *En Artificial intelligence as a disruptive technology: economic*

- transformation and government regulation*, editado por Rosario Girasa, 105-146. Berlín: Springer. Doi: 10.1007/978-3-030-35975-1_4.
- Graham, Jamie. 2023. «The dark web and human trafficking». *Doctoral Dissertations and Projects*, marzo 21. Acceso el 2 de marzo de 2025: <https://digitalcommons.liberty.edu/doctoral/4215>.
- Gstrein, Oskar J., Noman Haleem y Andrej Zwitter. 2024. «General-purpose AI regulation and the European Union AI Act». *Internet Policy Review* 13(3): 1-26. Doi: 10.14763/2024.3.1790.
- Hendrik, Elmert. 2018. *From fishing to phishing - University of Twente Research Information*. University of Twente. Acceso el 20 de febrero de 2025: <https://research.utwente.nl/en/publications/from-fishing-to-phishing/>.
- Hickle, Kristine. 2017. «Victims of sex trafficking and online sexual exploitation». En *Cybercrime and its victims*, editado por Elena Martellozzo y Emma Jane, 94-107. Londres: Routledge.
- Hong, Seung P. 2023. «The light and shade of generative AI in crime». *The Korean Society of Private Security* 22(5): 117-42. Doi: 10.56603/jksp.2023.22.5.117.
- ICAT. 2024. *Annual Report 2024*. Acceso el 10 de marzo de 2025. <https://migrantprotection.iom.int/en/resources/report/icat-2024-annual-report#:~:text=In%202024%2C%20ICAT%20focused%20on,trafficking%20responses%20in%20crisis%20contexts>.
- Ijiga, Amina, Enoch Aboi, Idoko Idoko, Lawrence Enyejo, y Micheal Odeyemi. 2024. «Collaborative innovations in artificial intelligence (AI): partnering with leading U.S. tech firms to combat human trafficking». *Global Journal of Engineering and Technology Advances* 18(3): 106-23. Doi: 10.30574/gjeta.2024.18.3.0046.
- Ijiga, Amina, Toyosi M. Olola, Lawrence A. Enyejo, Francis A. Akpa, Timilehin I. Olatunde y Frederick I. Olajide. 2024. «Advanced surveillance and detection systems using deep learning to combat human trafficking». *Magna Scientia Advanced Research and Reviews* 11(1): 267-86. Doi:10.30574/msarr.2024.11.1.0091.
- Jeong, Doowon. 2020. «Artificial intelligence security threat, crime, and forensics: taxonomy and open issues». *IEEE Access* 8: 184560-74. Doi: 10.1109/ACCESS.2020.3029280.
- Kejriwal, Mayank y Pedro Szekely. 2022. «Knowledge graphs for social good: an entity-centric search engine for the human trafficking domain». *IEEE Transactions on Big Data* 8(3): 592-606. Doi: 10.1109/TBDATA.2017.2763164
- Khanal, Shushant. 2020. «Human trafficking in Nepal: can big data help?». *Undergraduate Research Journal* 24(1): 41-49. Acceso el 26 de febrero de 2025: <https://openspaces.unk.edu/undergraduate-research-journal/vol24/iss1/5>.
- King, Thomas C., Nikita Aggarwal, Mariarosaria Taddeo y Luciano Floridi. 2020. «Artificial intelligence crime: An interdisciplinary analysis of foreseeable threats and solutions». *Science and Engineering Ethics* 26(1): 89-120. Doi: 10.1007/s11948-018-00081-0.

- Kupriianova, Larysa y Daryna Kupriianova. 2023. «The AI in the porn industry of social media: human replacement or precursor for growing the sexual violence and human trafficking indicators?» *Collection of Scientific Papers SCIENTIA* 6, 75-82.
- Latonero, Mark. 2011. «Human trafficking online: The role of social networking sites and online classifieds». *SSRN Scholarly Paper* n. 2045851. Doi: 10.2139/ssrn.2045851.
- Laux, Johann, Sandra Wachter y Brent Mittelstadt. 2024. «Trustworthy artificial intelligence and the European Union AI Act: On the conflation of trustworthiness and acceptability of risk». *Regulation & Governance* 18(1): 3-32. Doi: 10.1111/rego.12512.
- Lazarus, Suleman, Mina Chiang y Mark Button. 2025. «Assesing human trafficking and cybercrime intersections through survivor narratives». *Deviant Behavior* 47(7): 1252-1269.
- LeBaron, Genevieve y Andrew Crane. 2018. «Methodological challenges in the business of forced labour». En *Researching forced labour in the global economy: methodological challenges and advances*, editado por Genevieve LeBaron. Londres: British Academy. Doi: 10.5871/bacad/9780197266472.003.0002.
- Leng, Olivia, Shereen Khan y Rohani Abd Rahim. 2014. «Internet: The double-edged sword of trafficking of women in Malaysia». *Pertanika Journal* 22: 149-60.
- Marinus Analytics. s.f. *Traffic Jam*. Acceso el 25 de febrero de 2025: <https://www.marinusanalytics.com/traffic-jam>.
- Marion, Nancy E. y Kimberly J. Hufgard. 2025. *The politics of combating human trafficking in the United States: A policy perspective*. Londres: Taylor & Francis.
- Mehra, Ananya V. y Gazala Sharif. 2024. «Legal framework and international cooperation in combatting human trafficking». *International Journal For Multidisciplinary Research* 6(2). Doi: 10.36948/ijfmr.2024.v06i02.18087.
- Microsoft. s.f. *PhotoDNA*. Acceso el 25 de febrero de 2025: <https://www.microsoft.com/en-us/photodna>.
- Moldovan, Ramona M. 2011. «Human trafficking in cyberspace». *The Juridical Current* 46: 86-92.
- Moser, Maddison M. 2021. «Human trafficking and online platform liability». *University of Toledo Law Review* 53: 159-181.
- Naheem, Mohammed A. 2020. «Do cryptocurrencies enable and facilitate modern slavery?» *Journal of Money Laundering Control* 24(3): 491-501. Doi: 10.1108/JMLC-07-2020-0073.
- Nour, Nika y Julia Gelfand. 2022. «Deepfakes: a digital transformation leads to misinformation». *GL-Conference Series: Conference Proceedings* 11.
- OIM. 2024. *World Migration Report 2024*. Acceso el 28 de febrero de 2025: <https://publications.iom.int/books/world-migration-report-2024>.
- Orantes, Marlon. 2018. *Leveraging machine learning and artificial intelligence to combat human trafficking*. Utica College. Acceso el 27 de febrero de

- 2025: <https://www.proquest.com/docview/2160987666?pq-origsite=gscholar&fromopenview=true&sourcetype=Dissertations%20&%20Theses>.
- Perussi, Jordana M. y Paulo C. Correa. 2024. «O uso da inteligência artificial no combate ao tráfico de pessoas». *Latin American Human Rights Studies* 4: 1-14. Doi: 10.5216/lahrs.v4.81297.
- Pittsburgh Technology Council. s.f. *40 Stories: Cara Jones and Erick Rigby of Marinus Analytics*. Acceso el 25 de febrero de 2025: https://www.pghtech.org/news-and-publications/Marinus_analytics_1.
- Polaris. 2018. *On-ramps, intersections, and exit routes: A roadmap for systems and industries to prevent and disrupt human trafficking*. Washington D.C.: Polaris.
- Popov, Konstantin y Mattia Masolletti. 2021. «Withdrawn: human trafficking: Trends and methods of counteraction». Preprint OSF, diciembre 10. Acceso el 1 de marzo de 2025: https://osf.io/j94qa_v1.
- Portnoff, Rebecca S., Danny Y. Huang, Periwinkle Doerfler, Sadia Afroz y Damon McCoy. 2017. «Backpage and bitcoin: Uncovering human traffickers». *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*. New York, 13 agosto, 1595-604. Doi: 10.1145/3097983.3098082.
- Raets, Sigrid y Jelle Janssens. 2018. «Trafficking & technology: The role of digital communication technologies in the human trafficking business». *Linking Organized Crime and Cybercrime (LOCC 2018): Presentations*. Acceso el 27 de febrero de 2025: <http://hdl.handle.net/1854/LU-8601401>.
- Rentzsch, Viola. 2021. *Human trafficking 2.0 the impact of new technologies*. Acceso el 28 de febrero de 2025: <https://hdl.handle.net/10566/10306>.
- Rifki, Sayid. 2023. «The fusion of blockchain, pornography and human trafficking in a global digital dragnet that forms the online child sex trafficking». *Russian Law Journal* 11(5s): 5s. Doi: 10.52783/rlj.v11i5s.891.
- Ríos, Ángeles de los. 2025. «Derechos humanos e inteligencia artificial». *Revista de Derecho, Empresa y Sociedad* 25: 179-87.
- Runyon, Natalie. 2025. *AI puts spotlight on victim identification in fight against domestic minor sex trafficking*. Thomson Reuters Institute, enero 24. Acceso el 27 de febrero de 2025: <https://www.thomsonreuters.com/en-us/posts/human-rights-crimes/spotlight-trafficking-victim-identification/>.
- Sarkar, Siddhartha. 2024. *Use of social networking technology in sex trafficking*. Londres: Lexington Books. Doi: 10.5771/9781666954777.
- Sharma, Rohan, Bhavin Jawade, Akshay Agarwal, Srirangaraj Setlur y Nalini Ratha. 2023. «Attention guided multi-attribute architecture for deepfake detection». *2023 IEEE Western New York Image and Signal Processing Workshop*, 1-4. Doi: 10.1109/WNYISPW60588.2023.10349650.
- Shivani. 2024. «Dark web and its ramifications». *International Journal for Multidisciplinary Research* 6(5): 1-5. Doi: 10.36948/ijfmr.2024.v06i05.28918.
- Shelley, Louise. 2010. *Human trafficking: A global perspective*. Cambridge: Cambridge University Press.

- Singh, Aditya. 2020. *Photo DNA*. mayo 26. Acceso el 2 de marzo de 2025: <https://repository.iiitd.edu.in/xmlui/handle/123456789/891>
- Spice, Byron. 2019. «CMU-developed software aids sting operation against sex traffickers». Carnegie Mellon School of Computer Science, febrero 21. Acceso el 28 de marzo de 2025: <https://www.cs.cmu.edu/news/2019/cmu-developed-software-aids-sting-operation-against-sex-traffickers>.
- Spotlight. s.f. *The issue*. Acceso el 25 de febrero de 2025: <https://www.spotlight.ngo>.
- Steinebach, Martin. 2023. «An analysis of PhotoDNA». *Proceedings of the 18th International Conference on Availability, Reliability and Security*. Agosto 29, 1-8. Doi: 10.1145/3600160.3605048
- Steinebach, Martin. 2024. «Robustness and collision-resistance of PhotoDNA». *Journal of Cyber Security and Mobility*, abril 9, 541-564. Doi: 10.13052/jcsm2245-1439.1339.
- Stylianou, Abby, Jessica Schreier, Richard Souvenir y Robert Pless. 2017. «TraffickCam: crowdsourced and computer vision based approaches to fighting sex trafficking». *2017 IEEE Applied Imagery Pattern Recognition Workshop (AIPR)*, octubre, 1-8. Doi: 10.1109/AIPR.2017.8457947.
- Stylianou, Abby, Richard Souvenir y Robert Pless. 2019. *TraffickCam: Explainable image matching for sex trafficking investigations*. Office of Justice Programs. No. 254596. U.S. Department of Justice. Acceso el 25 de marzo de 2025: <https://www.ojp.gov/ncjrs/virtual-library/abstracts/traffickcam-explainable-image-matching-sex-trafficking>.
- Susanti, Destina R. y Rina A. Prastyanti. 2024. «Law enforcement against international human trafficking». *International Journal of Law and Society* 1(2): 142-52. Doi: 10.62951/ijls.v1i2.33.
- TAHub. s. f. *Traffic Analysis Hub*. Acceso el 25 de febrero de 2025: <https://www.traffikanalysis.org>.
- TraffickCam. s.f. *TraffickCam*. Acceso el 20 de febrero de 2025: <https://traffickcam.com/>.
- Triplett, William J. 2024. «Artificial intelligence, cybersecurity, and human trafficking networks». *Cybersecurity and Innovative Technology Journal* 2(2): 2. Doi: 10.53889/citj.v2i2.556.
- UNODC. 2020. *Global Report on Trafficking in Persons 2020*. Acceso el 20 de febrero 2025: <https://www.unodc.org/unodc/en/data-and-analysis/glotip-2020.html>
- UNODC. 2024. *The 2024 Global Report on Trafficking in Persons 2024*. Acceso el 20 de febrero 2025: <https://www.unodc.org/unodc/en/data-and-analysis/glotip.html>
- U.S. Department of State. 2024. *Trafficking in Persons Report 2024*. Acceso el 20 de febrero 2025: <https://www.state.gov/reports/2024-trafficking-in-persons-report/>