PROYECTO FIN DE GRADO

TÍTULO: El Impacto de la Inteligencia Artificial en la Identificación y Prevención del Delito

AUTOR: Estela Alejandra Ortiz Alarcón

TUTOR:
SEBASTIÁN LINARES LEJARRAGA

GRADO EN CRIMINOLOGÍA

FACULTAD DE CIENCIAS SOCIALES Y COMUNICACIÓN

UNIVERSIDAD EUROPEA DE MADRID

DEDICATORIA

A mi madre, por ser mi mayor ejemplo de fortaleza y dedicación, por tu amor incondicional, tu apoyo constante y por enseñarme que no hay meta inalcanzable cuando se trabaja con el corazón.

A mi esposo, por estar siempre a mi lado, por tu comprensión y por ser mi mayor pilar en este camino. Gracias por tu paciencia, tu amor y por recordarme cada día que juntos podemos superar cualquier desafío, este logro también es tuyo.

A mi amiga y compañera María José Portillo Gonzalez, que empezamos este camino juntas, compartiendo no solo el esfuerzo, sino también las emociones, las caídas y los logros. Gracias por tu cercanía, por tu fuerza y por convertir este proceso en una experiencia que no olvidaré. Este trabajo es reflejo de nuestra constancia y del esfuerzo compartido.

AGRADECIMIENTOS

Deseo manifestar mi más profundo agradecimiento a la Universidad Europea de Madrid por proporcionarme la capacitación, los medios y el ambiente académico requeridos para la realización de este trabajo.

Extiendo un especial agradecimiento a mi tutor, Sebastián Linares Lejarraga, por su valiosa orientación, dedicación y comentarios que enriquecieron cada etapa del proyecto.

Asimismo, agradezco a las instituciones y fuentes de información que facilitaron datos relevantes, así como a todas las personas que contribuyeron directa o indirectamente al desarrollo de este trabajo.

Finalmente, quiero manifestar mi profundo agradecimiento al Dr. Jorge Ramiro Pérez, cuyo apoyo constante, compromiso y cercanía fueron fundamentales para culminar este proyecto. Sin él, esto no hubiera sido posible.

Resumen

El uso de la inteligencia artificial (IA) en la criminología presenta la oportunidad de implementar tácticas innovadoras para prevenir y luchar contra el delito. El presente trabajo de investigación busca examinar la influencia de la Inteligencia Artificial en la detección y prevención del delito, basándose en casos reconocidos a nivel internacional, como EncroChat, Matrix y Ghost. Además del uso de instrumentos predictivos por parte de las Fuerzas y Cuerpos de Seguridad, como el Sistema de Anticipación del Delito (CAS) en el caso de los Países Bajos. Este análisis de casos y de herramientas de inteligencia artificial permite aplicaciones fundamentales en el análisis de datos en masa, la predicción de delitos y la colaboración internacional, lo cual ha probado ser crucial para desmantelar redes delictivas.

Además se observan los retos éticos y técnicos vinculados al uso de la IA como herramienta para la prevención y detección del delito, como la discriminación por algoritmos, la posibilidad de la invasión de la privacidad y una posible falta de claridad en los sistemas. Se analiza el marco jurídico relevante a través del estudio de regulaciones como el AI Act y el GDPR, las cuales orientan el desarrollo responsable de la inteligencia artificial como nueva tecnología. También debe fortalecerse la normativa, capacitar a las fuerzas de seguridad en el uso ético de esta herramienta y promover la colaboración internacional, para así garantizar el respeto de los derechos fundamentales al utilizar la IA como método de mejora en la seguridad ciudadana.

Palabras-clave: Vigilancia predictiva, Algoritmos predictivos, Seguridad pública, Protección de datos, Cooperación internacional.

Abstract

The use of artificial intelligence (AI) in criminology presents the opportunity to implement innovative tactics to prevent and combat crime. This research paper seeks to examine the influence of AI on crime detection and prevention, based on internationally recognized cases such as EncroChat, Matrix, and Ghost. It also examines the use of predictive tools by law enforcement agencies, such as the Crime Anticipation System (CAS) in the Netherlands. This analysis of cases and AI tools enables fundamental applications in big data analysis, crime prediction, and international collaboration, which have proven crucial in dismantling criminal networks.

It also examines the ethical and technical challenges associated with the use of AI as a tool for crime prevention and detection, such as algorithmic discrimination, the potential for privacy invasion, and a potential lack of clarity in systems. The relevant legal framework is analyzed through a study of regulations such as the AI Act and the GDPR, which guide the responsible development of artificial intelligence as a new technology. Regulations must also be strengthened, law enforcement agencies trained in the ethical use of this tool, and international collaboration promoted to ensure respect for fundamental rights when using AI as a method to improve citizen security.

Keywords: Predictive surveillance, Predictive algorithms, Public safety, Data protection, International cooperation.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE SIGLAS Y ABREVIATURAS

Sigla	**Inglés**	**Español**
AI ACT	Artificial Intelligence Act	Ley de Inteligencia Artificial
DL	Deep Learning	Aprendizaje Profundo
IA	Artificial intelligence	Inteligencia Artificial
ML	Machine Learning	Aprendizaje Automático
NLP	Natural Language Processing	Procesamiento del Lengua
ODS	Sustainable Development Goals	Objetivos de Desarrollo Sostenible
OSINT	Open Source Intelligence	Inteligencia de Fuentes Abiertas
PNUD	United Nations DEvelopment Program	Programa de las Naciones Unida para el Desarrollo
RGPD	The General Data Protection Regulation	El Reglamento General de Protección de Datos

Fuente: Elaboración propia a partir de Traducciones y definiciones adaptadas de Decide Soluciones (2023).

1. INTRODUCCIÓN

1.1 Planteamiento del problema

En los últimos años, la inteligencia artificial ha empezado a meterse de lleno en campos donde antes ni se la imaginaba, como el de la seguridad o el de la justicia penal. Su principal ventaja, al menos una de las más notables, es que puede manejar cantidades enormes de información y detectar relaciones o patrones que a simple vista no se detectan. Gracias a eso, se ha empezado a usar para todo tipo de tareas: desde revisar grabaciones o imágenes casi en tiempo real, hasta señalar movimientos raros en redes informáticas o intentar prever delitos antes de que ocurran, basándose en datos previos. No es ciencia ficción; ya está pasando (Aguilar Cabrera, 2024).

Ahora bien, cuando se empieza a aplicar la inteligencia artificial en áreas como la justicia o la seguridad, no todo es tan sencillo. Aparecen bastantes retos, tanto técnicos como éticos y legales. Un problema que destaca bastante es la falta de una regulación clara y común entre países. Algunos países ya han creado leyes más o menos específicas para regular el uso de la inteligencia artificial en estos contextos. Sin embargo, muchos otros todavía no han dicho nada al respecto, esta falta de regulación genera muchas dudas. No está claro hasta dónde se puede llegar con esta tecnología ni qué consecuencias podría haber sobre derechos fundamentales, como el derecho a la privacidad o a un trato justo ante la ley.

Un problema serio que conviene mencionar es que la inteligencia artificial aprende de información que ya existe, y claro, eso significa que también puede arrastrar errores del pasado. De hecho, no solo los arrastra: a veces los hace más grandes. Esto terminará afectando sobre todo a grupos que ya tienen difícil su situación (Basu, 2020), y la verdad, pone en cuestión algo tan básico como que todas las personas sean tratadas por igual dentro del sistema judicial.

Si bien, la cuestión de la privacidad es otro tema delicado, tecnologías como el reconocimiento facial o los sistemas de vigilancia automática generan bastante inquietud por cómo podrían usarse. Si no se establecen límites claros, tratar grandes cantidades de datos personales puede derivar en situaciones que pongan en peligro derechos fundamentales, como la presunción de inocencia, la protección de la información personal o el acceso a un juicio justo. Como advierten Peña Torres y Martabit Sagredo (2024), la falta de criterios éticos y

marcos normativos adecuados hace que aumenten los riesgos, sobre todo en contextos en los que no hay mecanismos sólidos de control, transparencia ni rendición de cuentas.

Tomando en cuenta los aspectos mencionados anteriormente, se debe estudiar la manera en que se está aplicando la inteligencia artificial en situaciones reales y no quedarse únicamente en un estudio teórico. La presente investigación busca analizar tres casos a nivel internacional (EncroChat, Matrix y la Operación Ghost) en los cuales se ha utilizado Inteligencia Artificial para desmantelar redes delictivas. Además se realiza un estudio de la herramienta predictiva Sistema de Anticipación del Delito (CAS) creada en los Países Bajos. El uso de casos reales y herramientas de IA existentes en el estudio facilita el análisis del efecto de estas tecnologías en la criminología, además de señalar las ventajas y peligros que su uso brinda a los derechos y libertades de las personas.

Hipótesis: Si se implementa respetando los marcos legales vigentes y principios éticos fundamentales, la inteligencia artificial puede convertirse en una herramienta eficaz para proponer soluciones y mecanismos de prevención y detección del delito, sin comprometer los derechos fundamentales de las personas.

1.2 Pregunta de investigación

¿Es posible que la inteligencia artificial aporte herramientas y propuestas deficientes para la detección y prevención del crimen sin poner en riesgo los derechos esenciales de los individuos?

1.3 Objetivos del trabajo

1.3.1 Objetivo general

Examinar el efecto de la inteligencia artificial en la detección y prevención del crimen, evaluando su efectividad, peligros y posibilidades en el ámbito de la seguridad pública, sin vulnerar los derechos fundamentales.

1.3.2 Objetivos específicos

1. Analizar las aplicaciones más relevantes de la inteligencia artificial para identificar patrones delictivos y prevenir acciones delictivas.

2. Determinar los desafíos éticos y jurídicos vinculados al empleo de la Inteligencia Artificial en el sector de la justicia y la seguridad.
3. Examinar las tecnologías más empleadas en la aplicación de Inteligencia Artificial enfocada en la lucha contra el crimen.
4. Sugerencias para un uso ético, responsable y eficaz de la inteligencia artificial en el campo de la criminología y la seguridad ciudadana.

1.4 Justificación: La relevancia, originalidad y contribución científica al conocimiento académico

El tema de la inteligencia artificial no solo está muy presente en el mundo actual, sino que también conecta con muchas de las preguntas que han ido surgiendo a lo largo de la carrera. En estos últimos años, he visto cómo la tecnología se ha ido metiendo poco a poco en todos los aspectos de nuestra vida diaria, y la criminología no queda al margen de ese cambio. La inteligencia artificial, que hace poco parecía cosa del futuro, ya forma parte de muchas decisiones que tomamos o que se toman por nosotros: aparece en las redes sociales, en los sistemas de vigilancia y también en herramientas que utilizan cuerpos de seguridad.

Es muy importante, desde el punto de vista de la criminología, observar de forma crítica lo que supone este avance para la seguridad pública. Es obvio que la inteligencia artificial tiene cosas positivas que aportar, pero debemos preguntarnos qué precio estamos dispuestos a pagar para tener acceso a estos avances. ¿Estamos preparados para enfrentar los dilemas éticos que conlleva? ¿Qué nivel de protección tienen los ciudadanos ante un nuevo sistema automático que es el que toma decisiones que pueden afectarles directamente?

El presente trabajo busca aportar al debate académico combinando teoría y aplicación a través del estudio de casos prácticos, sin perder de vista la dimensión humana de los problemas abordados, esto quiere decir analizar cómo estos algoritmos y datos afectan a las personas. Es por eso que este estudio busca realizar una contribución tanto técnica como ética y social al aportar ideas que pueden ser útiles para el diseño de políticas más responsables respecto al uso de la inteligencia artificial y conscientes de los derechos de los ciudadanos.

En este sentido, la investigación también se alinea con los Objetivos de Desarrollo Sostenible (ODS) establecidos por la Agenda 2030 de las Naciones Unidas, en particular con los ODS 9, 10 y 12, orientados a la innovación y el desarrollo de infraestructuras resilientes,

la reducción de la desigualdad y la producción y consumo responsable, respectivamente. El uso de la inteligencia artificial en criminología debe abordarse desde una perspectiva crítica y responsable, no por ser una necesidad académica y profesional, sino también un compromiso con la construcción de sistemas de seguridad más éticos, equitativos y sostenibles (Programa de las Naciones Unidas para el Desarrollo, 2015).

2. MARCO TEÓRICO

2.1 Historia de la IA en Criminología: Línea de Tiempo de la Evolución de Tecnologías Aplicadas al Crimen

El progreso de la inteligencia artificial (IA) ha revolucionado de manera significativa el área de la criminología y la seguridad pública, desde sus bases teóricas hasta su uso práctico en la prevención, identificación y lucha contra el crimen. En las décadas recientes, estas tecnologías han transformado radicalmente las tácticas policiales, propulsadas por progresos en aprendizaje automático, análisis de datos y sistemas de predicción.

Durante los años 50, la Inteligencia Artificial empezó a establecerse como una disciplina, sobresaliendo la Conferencia de Dartmouth en 1956, en la que se estableció el concepto de "inteligencia artificial" (McCarthy, 2006). A pesar de que en esa época no existía un uso directo en la criminología para la inteligencia artificial, fue entonces que se sentaron las bases para la creación de los algoritmos y sistemas de aprendizaje que se aplicarían al estudio del delito en el futuro.

En las décadas de 1970 y 1980 aparecieron los primeros sistemas de expertos, creados para respaldar la toma de decisiones en áreas como la medicina y la protección. Simultáneamente, se pusieron en marcha bases de datos digitales que agrupaban historiales delictivos, simplificando el acceso inmediato a la información para los equipos de policía (Perry, McInnis, Price, Smith y Hollywood, 2013). Estos avances establecieron el comienzo de la detección sistemática de patrones delictivos.

El inicio de la década de 1990 supuso un crecimiento en la utilización de bases de datos y los primeros análisis predictivos en el campo criminológico. Iniciativas como el Centro Nacional de Información de Delincuencia (NCIC) en Estados Unidos y la estrategia CompStat en Nueva York implementaron estudios estadísticos sofisticados para identificar patrones

delictivos y maximizar la distribución de recursos de la policía (Police, 2024). Estas herramientas establecieron un hito hacia estrategias fundamentadas en información.

Desde el año 2000, el aprendizaje automático se estableció como un instrumento crucial en el campo de la criminalística. Comenzaron a implementarse algoritmos para reconocer patrones complejos en los sistemas de reconocimiento facial y videovigilancia inteligentes, creados para identificar conductas sospechosas en tiempo real, lo cual permitió la implementación masiva de la Inteligencia Artificial en la seguridad ciudadana (Europol, 2024).

Durante los años 2010, el crecimiento del big data y las herramientas predictivas basadas en Inteligencia Artificial modificaron aún más el escenario. Un caso reconocido es PredPol, una iniciativa de la Policía de Los Ángeles en 2012, que demostró cómo modelos de aprendizaje automático podían prever delitos en áreas concretas (Perry, 2013). Simultáneamente, tecnologías como la biometría y el reconocimiento de rostros se normalizaron en aeropuertos y grandes acontecimientos, fortaleciendo la seguridad preventiva (Financial Times, 2024).

Desde el año 2020 hasta el presente, la inteligencia artificial ha adquirido nuevas dimensiones a través de aplicaciones sofisticadas y operaciones coordinadas a nivel internacional. Eventos como la desintegración de EncroChat en 2020, la operación Ghost en 2024 y la intervención más reciente sobre Matrix demuestran la habilidad de la Inteligencia Artificial para interceptar comunicaciones encriptadas, manejar grandes cantidades de información y coordinar operaciones multinacionales en tiempo real (Europol, 2020; Europol, 2024).

Instrumentos como el Sistema de Anticipación del Delito (CAS) en los Países Bajos han ayudado a disminuir la delincuencia en áreas de riesgo a través del estudio de datos históricos y actuales con fines predictivos (Politie, 2021). Se espera que en el futuro la Inteligencia Artificial en criminología siga su progreso dentro de marcos legales como la Ley de IA y que esto, junto al avance de tecnologías éticas, reduzca las discriminaciones algorítmicas y fomente la transparencia (Unión Europea, 2021). Estas innovaciones potenciarán la colaboración global y facilitarán el enfrentamiento de nuevos desafíos, como el crimen cibernético y la utilización ilegal de la Inteligencia Artificial por parte de organizaciones delictivas (European Commission, 2021).

2.2 La inteligencia artificial:

La Inteligencia Artificial (IA) se ha establecido como un campo clave en el progreso tecnológico y científico actual. Desde sus primeras ideas hasta las implementaciones contemporáneas, ha sido objeto de varias definiciones y perspectivas. En términos operativos, la Inteligencia Artificial se puede definir como el área de estudio que aspira a crear sistemas capaces de llevar a cabo tareas que demandan inteligencia humana, que incluyen la percepción, el razonamiento, la planificación, el aprendizaje y la toma de decisiones (Russell y Norvig, 2020).

Su relevancia se basa en su habilidad para manejar grandes cantidades de información, identificar patrones complejos y producir soluciones innovadoras a problemas de variados tipos. En este contexto, uno de los propósitos fundamentales de la Inteligencia Artificial es la creación de máquinas intelectuales, o sea, sistemas que no solo replican la conducta humana, sino que también tengan la habilidad de ajustarse al ambiente y potenciar su rendimiento a partir de la experiencia obtenida.

Russell y Norvig (2020), en su influyente obra *Artificial Intelligence: A Modern Approach*, proponen una clasificación teórica que distingue cuatro enfoques fundamentales para entender la evolución de la inteligencia artificial: primero los sistemas que piensan como humanos, centrados en la simulación de los procesos cognitivos mediante modelos computacionales de aprendizaje y toma de decisiones, los segundos sistemas que actúan como humanos, una perspectiva inspirada en la capacidad de las máquinas para replicar el comportamiento inteligente a través de pruebas como el Test de Turing, que mide la habilidad de un sistema para generar respuestas indistinguibles de las producidas por una persona (Turing, 1950), los penúltimos sistemas que piensan racionalmente, basados en el uso de lógica formal y razonamiento deductivo mediante reglas estructuradas y modelos matemáticos y por último sistemas que actúan racionalmente, representados por agentes inteligentes capaces de maximizar su desempeño a partir del análisis de información obtenida del entorno y ajustar su comportamiento en función de objetivos específicos.

Tras estas visiones teóricas, la inteligencia artificial contemporánea se basa en tecnologías más sofisticadas como el aprendizaje automático y el aprendizaje profundo (Goodfellow, Bengio y Courville, 2016). En resumen, el aprendizaje automático opera de manera similar a la forma en que un individuo adquiere conocimientos de la experiencia. Por

ejemplo, si alguien quiere aprender a reconocer caras va confundirse al principio, pero con el tiempo empieza a acertar cada vez más, tras ver muchos rostros distintos. La IA hace algo similar: analiza grandes cantidades de datos, se equivoca, pero va ajustando sus criterios para mejorar sus decisiones. Así, sin necesidad de que un programador le diga exactamente qué hacer, puede aprender por sí misma a reconocer patrones y adaptarse a nuevas situaciones.

Estas técnicas permiten a los sistemas aprender automáticamente a partir del análisis de grandes volúmenes de datos, superando las limitaciones de los antiguos sistemas expertos, que se basan en estructuras lógicas predefinidas del tipo “si ocurre X, entonces hacer Y”. En contraste con los modelos convencionales, que se ajustaban únicamente a normas preestablecidas por los programadores, los algoritmos modernos incrementan su exactitud mediante un proceso de prueba y error, modificando progresivamente sus propios "criterios internos" para disminuir la discrepancia entre lo que anticipan y lo que sucede en realidad, con la finalidad de reducir la discrepancia entre las predicciones y los resultados obtenidos. Así, potencian su habilidad para reconocer y extender patrones complejos sin requerir una codificación explícita.

Las metodologías basadas en machine learning y deep learning han transformado el campo de la inteligencia artificial, impulsando grandes avances en áreas como la visión por computadora, el procesamiento del lenguaje natural y la robótica. Gracias al uso de redes neuronales artificiales, que permiten a estos sistemas descubrir relaciones entre datos que no serían fáciles detectables a simple vista, realizar inferencias precisas y adaptarse progresivamente a distintos contextos, lo que amplía significativamente sus posibilidades de aplicación en sectores como la seguridad, la salud o la justicia penal (LeCun, Bengio y Hinton, 2015).

Hablamos de máquinas que no solo siguen instrucciones fijas, sino que aprenden y mejoran con el tiempo, adaptándose a nuevas situaciones sin necesidad de intervención constante, permitiendo el avance de modelos con mayor independencia, habilidad para adaptarse y mejora constante. Pese a estos progresos, todavía no se ha logrado lo que se denomina inteligencia artificial general (AGI), o sea, un tipo de Inteligencia Artificial que pueda emular el conjunto integral de las funciones cognitivas humanas.

De acuerdo con Bostrom (2014), el desarrollo de una AGI supone no solo un reto tecnológico nunca antes visto, sino también un reto moral y regulatorio de gran envergadura, al

generar cuestionamientos acerca de su dominio, sus restricciones y sus efectos en la humanidad.

2.3 Delincuencia en el entorno digital: Nuevas modalidades delictivas

La evolución de la tecnología digital ha transformado profundamente las dinámicas delictivas, dando lugar a nuevas manifestaciones criminales adaptadas al entorno virtual. Estos delitos, cada vez más complejos y difíciles de rastrear, representan un desafío creciente para las fuerzas de seguridad, tanto por su carácter transnacional como por su rápida propagación (Europol, 2024).

En el escenario español, el progreso de la cibercriminalidad ha sido particularmente relevante. De acuerdo con el Informe sobre Cibercriminalidad de la Policía Nacional (2023) que Juan José López Ossorio presentó en el Congreso de Criminología de la Universidad Europea de Madrid, se contabilizaron más de 470.000 crímenes digitales. Esto sitúa la tasa nacional en 9,6 crímenes digitales por cada mil residentes. Este dato refleja una duplicación del volumen delictivo digital respecto a 2019, marcando un crecimiento sostenido desde 2016 y evidenciando la consolidación del ciberespacio como un terreno prioritario de intervención criminológica.

Dentro de esta realidad, el fraude informático se ha posicionado como el ciberdelito más frecuente, alcanzando los 427.448 casos en 2023, lo que representa un abrumador 90,5 % del total de ciberdelitos registrados. Este fenómeno se ha visto alimentado por el auge del comercio electrónico y por prácticas como el phishing, la suplantación de identidad y las estafas en plataformas digitales. Su expansión no sólo tiene implicaciones económicas, sino también sociales y de seguridad, al comprometer la confianza ciudadana en el entorno digital.

A estas formas se añaden otras amenazas significativas, como el ciberacoso, especialmente frecuente en redes sociales y servicios de mensajería, que representa una forma de violencia digital que impacta seriamente en el bienestar emocional de las víctimas, especialmente los adolescentes. Este tipo de práctica puede expresarse mediante el desarrollo de contenidos agresivos producidos por la Inteligencia Artificial o la automatización del hostigamiento a través de bots.

El hurto de identidad sigue creciendo, promovido por el ingreso ilegal a bases de datos vulnerables y la aplicación de métodos de ingeniería social como el phishing y el spear

phishing. Mientras que el phishing implica el envío en masa de mensajes engañosos destinados a entidades legítimas para adquirir información personal, el spear phishing es una variante más selectiva y avanzada, donde los ciberdelincuentes personalizan el mensaje tras una investigación de la víctima, incrementando las posibilidades de éxito (Wolters Kluwer, 2022).

Una amenaza cada vez más relevante son los ciberataques dirigidos a infraestructuras críticas como redes eléctricas, hospitales o sistemas gubernamentales. Este tipo de delitos con potencial de impacto sistémico suelen ser perpetrados por grupos organizados de ciberdelincuentes o incluso por actores estatales con fines geopolíticos (Europol, 2020). A ello se suma la naturaleza descentralizada y anónima de las criptomonedas que ha facilitado nuevas formas de criminalidad, como las estafas de inversión, el ransomware o el lavado de dinero, y cuya investigación es cada vez más complicada por el fácil encubrimiento de los responsables.

Un ejemplo de estos ataques sistémicos es el apagón ocurrido el lunes 28 de abril de 2025, que dejó sin electricidad durante horas a millones de personas en España, Francia y Portugal. Aunque todavía no se ha confirmado su origen, se plantea la teoría de que eventos de esta magnitud podrían estar relacionados con ciberataques a infraestructuras críticas. Es por esto que, a pesar de que no exista confirmación de que este acontecimiento se tratase de un ciberataque, situaciones como esta permiten visibilizar el posible alcance de ataques coordinados e identificar la necesidad de los Estados de contar con mecanismos de prevención, respuesta y resiliencia.

El uso de inteligencia artificial con fines delictivos está creciendo de forma alarmante, tecnologías como los *deepfakes*, utilizadas en campañas de desinformación o extorsión, junto con bots automatizados que ejecutan ataques o manipulan el tráfico digital, plantean nuevos retos tanto técnicos como jurídicos (European Commission, 2021).

A esta evolución delictiva se suma una alerta reciente emitida por Europol sobre el uso reciente de IA por parte del crimen organizado. Según un artículo publicado en Wired (2025), las organizaciones criminales están comenzando a incorporar herramientas de IA generativa para ejecutar fraudes más sofisticados, creando identidades falsas mediante deepfakes, automatizar ataques de phishing e incluso manipular campañas de desinformación. Estas innovaciones tecnologías, que anteriormente estaban reservadas a entornos académicos o gubernamentales, ahora son accesibles en mercados ilegales, lo que incrementa notablemente su capacidad de causar daño.

Es importante destacar que la victimización digital también muestra significativas disparidades de género. De acuerdo con información policial, los hombres son los más afectados por fraudes en línea (87 %), mientras que las mujeres son las más afectadas por delitos sexuales digitales (66 %). Esta disparidad evidencia la necesidad de enfoques diferenciados en las estrategias de prevención y en la atención a las víctimas.

Ante este panorama cambiante y complejo, se vuelve imprescindible una respuesta estratégica que combine capacidad tecnológica con legitimidad institucional. No basta con crear instrumentos sofisticados de análisis y predicción; es crucial que estos se incorporen en un marco legal consistente, operativo y en concordancia con los valores democráticos. Sin embargo, la inteligencia artificial no debe ser vista meramente como una solución técnica, sino más bien como una herramienta que necesita constante supervisión humana, claridad en las operaciones y sistemas de control moral. Únicamente en estas circunstancias podrá fomentar la confianza social y establecerse como un instrumento de cambio en la batalla contra el crimen digital.

2.4 Aplicaciones de la IA en la criminología

La inteligencia artificial se ha convertido en una herramienta fundamental dentro de la criminología contemporánea, su capacidad para procesar enormes volúmenes de datos, identificar patrones ocultos y adaptarse en tiempo real ha transformado profundamente la manera en que se previenen y se investigan los delitos.

Uno de los usos más relevantes es su aplicación en el análisis de información masiva, gracias a la IA, hoy es posible detectar tendencias delictivas que antes pasaban desapercibidas. Por ejemplo, el estudio de movimientos financieros mediante algoritmos ha permitido identificar redes complejas de fraude y lavado de dinero. Un caso paradigmático fue la operación *EncroChat*, en la que las autoridades, con apoyo de Europol, lograron acceder a millones de mensajes cifrados utilizados por redes criminales internacionales, obteniendo miles de arrestos y la incautación de recursos ilícitos (Europol, 2024: págs. 12–13).

El uso de sistemas predictivos también está ganando relevancia en el ámbito de la prevención del delito por su uso en la creación de herramientas basadas en el análisis de datos históricos y del entorno. Estas capacidades permiten identificar zonas con mayor riesgo de actividad delictiva y detectar patrones para anticipar comportamientos peligrosos. Un ejemplo

de estas herramientas es el Crime Anticipation System (CAS), desarrollado en los Países Bajos, este sistema cruza información local y externa para ayudar a los agentes de las fuerzas de seguridad a organizar sus estrategias de intervención de forma más efectiva (Europol, 2024: págs. 15–16).

La identificación biométrica es otro campo que se ha desarrollado gracias la implementación de la IA, tecnologías como el reconocimiento facial o la lectura de huellas dactilares han mejorado la precisión en la identificación de personas sospechosas o desaparecidas. También permite establecer vínculos entre diferentes hechos delictivos, facilitando una investigación más profunda de las redes criminales organizadas (Europol, 2024: págs. 21–26).

En el ámbito de la investigación digital, la IA también desempeña un papel clave en la recuperación y el análisis de pruebas almacenadas en dispositivos electrónicos o redes sociales se ha vuelto mucho más eficiente gracias a herramientas como la visión por computadora. Estas han sido especialmente útiles en casos de gran sensibilidad, como los relacionados con la pornografía infantil o la explotación sexual, donde el volumen de material a revisar puede ser abrumador (Europol, 2024: pág. 20).

También se han desarrollado herramientas capaces de interpretar texto y lenguaje hablado mediante procesamiento de lenguaje natural (NLP). Esta tecnología permite analizar conversaciones en redes sociales o foros, detectar amenazas o comportamientos sospechosos y actuar de forma preventiva. En el ámbito del cibercrimen, este tipo de análisis ha mejorado notablemente la capacidad de reacción de las autoridades (Europol, 2024: págs. 18–19).

Cabe mencionar el papel de la inteligencia artificial en la automatización del análisis de fuentes abiertas y redes sociales, conocido como OSINT y SOCMINT. Estas herramientas son capaces de analizar grandes cantidades de datos no estructurados para detectar señales de alerta, como la difusión de propaganda extremista o la organización de actividades ilícitas (Europol, 2024: págs. 17–18).

Las aplicaciones mencionadas anteriormente reflejan la versatilidad de la inteligencia artificial en el ámbito de la criminología, además de demostrar su valor como una herramienta que puede contribuir a mejorar la seguridad al ser utilizada correctamente en el análisis preventivo en zonas de riesgo para así garantizar el bienestar de las personas.

2.5 Retos éticos y sociales del uso de la IA

La evolución de la inteligencia artificial (IA) en el campo de la criminología y la seguridad presenta retos significativos en términos éticos, jurídicos y sociales. Aunque estas tecnologías tienen un enorme potencial para identificar y prevenir el crimen, también suscitan inquietudes significativas respecto a tratos injustos originados por sistemas automatizados, la salvaguarda de la vida privada, la transparencia en los procedimientos tecnológicos y el respeto a los derechos fundamentales.

Uno de los componentes clave en la discusión es la categorización de los sistemas de Inteligencia Artificial (IA Act) de la Unión Europea, que cataloga los sistemas de IA en cuatro tipos: riesgo inaceptable, alto, limitado y mínimo. La mayor parte de los sistemas empleados en el campo de la seguridad pública, tales como el reconocimiento facial en tiempo real o los sistemas predictivos, son vistos como de "alto riesgo" y, por lo tanto, se rigen por requisitos rigurosos de transparencia, supervisión humana, seguimiento, valoración de impacto y calidad de la información.

La seguridad pública se encuentra en una posición delicada, ya que el AI Act prohíbe en general los sistemas de vigilancia biométrica masiva en espacios públicos, únicamente contempla excepciones para fines estrictamente definidos como la prevención de amenazas graves, la búsqueda de personas desaparecidas o la investigación de delitos particularmente graves, siempre bajo control judicial o administrativo previo (European Commission, 2021). Esto implica que las fuerzas de seguridad no pueden emplear libremente sistemas de videovigilancia con IA con fines preventivos, salvo que exista una justificación legal clara y proporcionada, y normalmente con autorización judicial.

La aplicación de Inteligencia Artificial en estas circunstancias generalmente implica la gestión de datos personales, especialmente datos biométricos y de localización, lo que genera desacuerdos con el Reglamento General de Protección de Datos 2016/679 (2016) (GDPR). Aunque esta normativa garantiza derechos como el acceso, rectificación, supresión y oposición, la Ley de Inteligencia Artificial permite excepcionar el consentimiento informado en determinadas circunstancias, como cuando el tratamiento de datos se realiza por motivo justificado. Este elemento ha sido criticado por su posible incertidumbre, ya que podría provocar interpretaciones amplias si no se aplica la normativa de forma más exacta.

Aún existe la posibilidad de que los sistemas aprendan y reproduzcan desigualdades sociales preexistentes, lo que puede traducirse en decisiones injustas que afectan de forma desproporcionada a determinados grupos sociales o étnicos. Ejemplos claros de ello son los algoritmos de predicción del crimen o los sistemas de reconocimiento facial, que han demostrado menor precisión en personas racializadas, aumentando el riesgo de identificaciones erróneas (Perry, 2013; Europol, 2024).

Para minimizar estos riesgos, la Ley de Inteligencia Artificial impone una serie de responsabilidades que comprenden la ejecución de evaluaciones anticipadas, auditorías externas, un análisis meticuloso de los datos y un monitoreo transparente de la forma en que se toman las decisiones. También plantea que los sistemas considerados de alto riesgo deben ser comprensibles para las personas, de forma que sus resultados no se presenten como una "caja negra" inexplicable, algo especialmente delicado cuando están en peligro cuestiones penales o judiciales.

La falta de claridad en los procesos automatizados sigue siendo uno de los grandes desafíos, por eso, resulta fundamental reforzar la responsabilidad de quienes desarrollan y aplican estas tecnologías, garantizar el derecho de las personas a recibir explicaciones sencillas sobre las decisiones que les afectan y asegurar que siempre haya margen para la intervención humana, sobre todo cuando están en juego derechos fundamentales.

2.6 Marco Normativo: Regulación de la IA en seguridad pública

El aumento en el uso de la inteligencia artificial en la criminología y la seguridad pública ha traído múltiples beneficios para la seguridad ciudadana, aunque también genera preguntas urgentes sobre cómo garantizar que estas tecnologías se utilicen de forma justa, responsable y respetuosa con los derechos de las personas. La evolución de la inteligencia artificial como herramienta en la criminología tiene una responsabilidad no sólo de innovar, sino también de establecer límites claros que eviten abusos, aseguren la transparencia en su funcionamiento y definan quién responde ante fallos en su uso.

Ante esta nueva responsabilidad resulta fundamental contar con marcos legales sólidos que regulen tanto el diseño como el uso de las Inteligencia Artificial como herramienta preventiva del delito. La regulación no solo protege a los ciudadanos, sino que también ofrece seguridad jurídica a quienes desarrollan o aplican estas tecnologías, pero a pesar de que en los

últimos años han surgido múltiples iniciativas a nivel nacional e internacional, todavía existen vacíos normativos y retos importantes en cuanto a su aplicación efectiva.

Regulación Internacional

AI Act (Unión Europea, 2024)

La Ley de Inteligencia Artificial de la Unión Europea (AI Act), vigente a partir de agosto de 2024, representa la primera ley completa sobre IA en los países miembros de la Unión Europea. Su meta es implementar un marco regulatorio que reduzca los peligros vinculados al empleo de estas tecnologías, fomentando la seguridad y la protección de los derechos fundamentales (Parlamento Europeo, 2024). El AI Act categoriza los sistemas de inteligencia artificial en cuatro grados de riesgo: cero, limitadísimo, elevado e ilegal. Las aplicaciones relacionadas con la seguridad pública son consideradas de riesgo elevado al utilizar el reconocimiento facial en tiempo real, los algoritmos de análisis de comportamiento o los sistemas predictivos, dado que estas herramientas pueden generar impactos considerables en derechos fundamentales como la privacidad, la libertad personal y la no discriminación.

El AI Act (2024) establece una serie de exigencias a lo largo de todo el ciclo de vida del sistema, entre ellas se incluyen la evaluación previa de riesgos, el uso de datos de entrenamiento representativos y equilibrados, la elaboración de documentación técnica que permita su auditoría y la trazabilidad de los procesos automatizados. También se requiere que los sistemas sean comprensibles para los operadores humanos como agentes policiales o jueces, lo que facilita una supervisión más transparente y responsable.

Una de las contribuciones más relevantes del reglamento es su énfasis en la supervisión humana. La inteligencia artificial debe complementar el juicio profesional, no sustituirlo, de modo que las decisiones automatizadas siempre deben ser sujetas a intervención y revisión humana, especialmente cuando afectan a derechos fundamentales. En cuanto a la vigilancia biométrica en espacios públicos, el AI Act (2024) la prohíbe de forma general, pero contempla excepciones en los casos de amenazas graves, desapariciones o delitos especialmente graves, siempre bajo autorización judicial o administrativa previa (European Commission, 2021).

Reglamento General de Protección de Datos (GDPR, Unión Europea, 2016)

El Reglamento General de Protección de Datos 2016/679 (2016) (GDPR) establece el estándar europeo para la protección de datos personales, proporcionando un marco legal que también se aplica al procesamiento de información sensible utilizando la IA. Su finalidad es garantizar que el uso de datos en sistemas de IA se realice éticamente y conforme a los principios de privacidad y seguridad (Unión Europea, 2016). Uno de sus pilares fundamentales es el consentimiento informado, el cual es un requisito indispensable para la recopilación y procesamiento de información personal, ya que asegura que los ciudadanos sean plenamente conscientes de cómo se utilizan sus datos.

La normativa impone límites a la recolección y tratamiento de datos, evitando el uso excesivo o innecesario de información que pueda comprometer la privacidad de los individuos. A su vez, esta garantía del derecho a la privacidad está relacionada con el derecho de acceso, rectificación y eliminación de datos, ya que otorga a los ciudadanos la capacidad de controlar su información personal y solicitar su modificación o eliminación.

Si bien estas disposiciones establecen un marco sólido para la gestión de datos a través de la IA, no abordan de manera específica los desafíos que surgen en su aplicación dentro del ámbito de la seguridad pública. Esta falta de regulación detallada abre las puertas a diversas interpretaciones y genera vacíos legales que pueden afectar la protección de los derechos individuales en contextos donde la inteligencia artificial desempeña un papel crítico (Unión Europea, 2016).

Retos en la Implementación de la IA en Seguridad Pública

El equilibrio entre la eficacia y el respeto a los derechos fundamentales en el contexto de la seguridad con respecto a la IA es particularmente sensible. Los sistemas de reconocimiento facial y los modelos predictivos han demostrado ser efectivos para prevenir el crimen y optimizar recursos. Pero si se abusa de ellos, pueden infringir derechos a la privacidad, igualdad o libertad individual.

Otro punto clave es la opacidad de varios algoritmos de IA. Frecuentemente se utilizan como verdaderas "cajas negras", ya que incluso los autores no pueden decir cómo se obtienen ciertos resultados. Esta falta de transparencia es especialmente preocupante en el ámbito legal, dado que las decisiones legales necesitan ser justificables y comprensibles para mantener la legitimidad y garantizar un tratamiento justo de todos los ciudadanos (Lipton, 2018).

Regulación Nacional: La Agencia Española de Supervisión de la Inteligencia Artificial (AESIA)

España ha emergido como pionera en el gobierno y supervisión de la IA con la creación de la Agencia Española para la Supervisión de la Inteligencia Artificial (AESIA) en 2022, la cual está alineada con la estrategia nacional para una IA confiable y ética y se transpondrá a las normas españolas para garantizar el cumplimiento de regulaciones (Ley de IA y RGPD) en el contexto nacional (Gobierno de España, 2022).

Una de sus principales responsabilidades es supervisar y restringir el uso de la IA, observando la implementación de la IA en los sectores privados y públicos de acuerdo con principios éticos y legales. También es crucial para los análisis de riesgo y auditoría, para prevenir algoritmos opacos o sesgados al promover la innovación responsable, desarrollando investigación en IA con sus estándares de seguridad y ética. España se fortalece como un referente en la regulación de la IA, con el objetivo de convertirse en el líder de la Unión Europea en la regulación de estas tecnologías, y sus acciones buscan combinar el progreso de la IA con la protección de los derechos fundamentales.

AESIA es una parte crítica de los esfuerzos de regulación de los sistemas de IA, particularmente en la categorización de sistemas de IA por niveles de riesgo. Esta categorización asegura que sea posible priorizar la supervisión de aquellas aplicaciones más perjudiciales para la protección de los derechos fundamentales y la seguridad pública. Por un lado, tecnologías de bajo riesgo que no incurren en riesgos para los derechos fundamentales (por ejemplo, para fines logísticos o administrativos como la asignación de fuerzas policiales) y las de alto riesgo, que podrían contribuir a reforzar estereotipos y estigmatizar muy rápidamente (por ejemplo, reconocimiento facial, tecnologías de análisis de datos, sistemas que identifican y predicen crímenes).

Además de su propósito regulatorio, AESIA ayuda a fomentar las normas éticas para determinar la aceptación y aplicación responsable de esta tecnología. La preservación de la privacidad, la prevención de sesgos que puedan reforzar desigualdades sociales o raciales, y la transparencia en la operación del sistema, pidiendo explicaciones claras de cómo se llegan a las decisiones automáticas, están entre sus prioridades.

En el ámbito de la criminología, AESIA aborda el uso de la IA en actividades de investigación y prevención del crimen. Evalúa los algoritmos para predecir zonas de riesgo, examina el uso del reconocimiento facial en términos de respeto a los derechos humanos y trabaja con socios europeos e internacionales en la lucha contra el crimen organizado en un mundo globalizado.

Aún existen dificultades en cuanto a la cooperación entre diferentes países, ya que a nivel internacional, no hay acuerdos regulatorios que estandaricen la gestión de redes y la operación centralizada del sistema, como el intercambio de datos y el desarrollo de una estrategia conjunta. Un problema más es el área gris legal cuando un sistema falla y los humanos están en la línea de fuego. La responsabilidad puede ser compartida entre el desarrollador y la entidad que despliega el sistema, pero esto no siempre es transparente y puede impactar la confianza pública en estas tecnologías (European Digital Rights, 2023).

Retos Actuales y Desafíos Futuros en la Supervisión de la IA

El establecimiento de la Agencia Española para la Supervisión de la Inteligencia Artificial (AESIA) es un paso en la dirección correcta en la regulación de la IA, aunque es necesario abordar varios impedimentos para que la AESIA sea completamente efectiva. Por lo tanto, el problema central es cómo podemos permitirnos suficientes expertos en contenido técnico (como yo) y líderes calificados para regular adecuadamente el flujo continuo de nuevas tecnologías. El desarrollo activo de estos y futuros sistemas de IA requerirá una inversión continua en capital humano, infraestructura y capacidades dedicadas para evaluar el impacto de los sistemas de IA en la seguridad pública y los derechos humanos.

Sobre el futuro, la interacción entre la Ley de IA y la regulación española podría provocar un choque regulatorio o crear áreas donde su existencia no pueda ser interpretada, lo que lleva a la necesidad urgente de esfuerzos de armonización para solucionar estos casos donde no surgen conflictos ni se distorsiona la implementación en las diferentes administraciones. La aparición del proceso de unificación de directrices éticas internacionales es también una oportunidad para que España apueste por convertirse en un referente en la nueva regulación de la IA a nivel internacional. Con AESIA, el país también puede iniciar proyectos dirigidos al establecimiento de directrices éticas compartidas y al diálogo con otros países y organizaciones internacionales.

Relación con el AI Act y su Impacto en Europa

La AESIA no existe de forma aislada, sino que junto con la Unión Europea es parte de una estrategia global para regular la inteligencia artificial. Su establecimiento refuerza la implementación de la AI ACT, promoviéndose como una agencia puente que garantiza la alineación con los estándares europeos en el uso de IA en España.

Para garantizar que los países cumplan con la ley en el campo de las tecnologías, podríamos proponer que la AESIA sea un modelo para que otros Estados Miembros formen sus propios organismos de auditoría. Ayudará a estandarizar las normas que gobiernan la IA en la UE, para facilitar el cumplimiento por parte de los desarrolladores y para que los usuarios confíen en su desarrollo y uso, al tiempo que se implementan las salvaguardias necesarias para asegurar que la IA satisfaga las demandas de sus ciudadanos.

La articulación de la AESIA como una entidad efectiva estará vinculada a su capacidad de adaptarse al progreso tecnológico, de armonizarse con regulaciones internacionales y de asegurar que el desarrollo de la inteligencia artificial en España se realice en línea con los principios de seguridad, justicia y responsabilidad que promueve la Unión Europea.

Impacto de la inteligencia artificial en la reducción del delito

La inteligencia artificial ha comenzado a desempeñar un papel importante en la prevención y control del delito. Su implementación en distintos contextos ha mejorado la eficiencia de las fuerzas de seguridad, especialmente en la gestión de recursos y en la identificación de amenazas potenciales. Sus contribuciones principales han incluido sus sistemas de predicción que hacen posible pronosticar áreas con un mayor riesgo de actividad delictiva. El uso de herramientas como PredPol en EE.UU., o el Sistema de Anticipación del Crimen (CAS) en los Países Bajos, ya ha resultado en una disminución del crimen, incluyendo robos y agresiones, al usar datos para asignar a la policía de forma óptima.

Las tecnologías de reconocimiento facial o vigilancia automatizada están llevando la identificación de sospechosos a nuevos límites, como en China. Pero tales avances, como todas las nuevas tecnologías, han suscitado preocupaciones sobre la privacidad. En el ámbito del crimen organizado, la inteligencia artificial ha mostrado su potencial para examinar e interpretar enormes bases de datos y descifrar mensajes codificados. Ejemplos como

EncroChat, Matrix y la Operación Ghost son evidencia de esto, con éxitos en la aplicación de la ley que incluyen una serie de arrestos masivos y confiscaciones de activos.

La IA no es la respuesta final, aún no, pero se puede ver el potencial. Sus virtudes necesitan ser realizadas en el contexto en el que se despliega, la regulación que la rodea y el imperativo de respeto por los derechos fundamentales. En este contexto, la experiencia holandesa emerge como un caso ejemplar de incorporación responsable y eficiente de estas tecnologías en políticas de prevención del terrorismo.

2.7 Teorías Criminológicas y su Conexión con la Inteligencia Artificial

La IA en el campo criminológico no surge de la nada: se basa en diversas teorías clásicas y modernas que explican por qué y cómo se comete el delito. Estas teorías ofrecen aparatos conceptuales básicos para entender los comportamientos, para guiar la recopilación de datos, los análisis y para estructurar enfoques con mayor respeto a los requisitos sociales y éticos.

En las siguientes secciones se planteara cómo las tendencias más importantes de las teorías criminológicas podrían ser reutilizadas en el diseño y despliegue de sistemas de IA en el contexto de la prevención del crimen. Este vínculo entre la teoría y la práctica tecnológica no solo enriquece las intervenciones de la policía y el trabajo social, sino que también promueve la reflexión sobre los límites, dilemas y riesgos de su implementación.

Según la Teoría de las Actividades Rutinarias (Cohen y Felson, 1979), el delito ocurre cuando se reúnen tres factores: un delincuente motivado, un objetivo adecuado y la falta de un guardián capaz. Un caso concreto es el sistema PredPol desplegado en Los Ángeles, que dirige las actividades policiales hacia donde se ha pronosticado el mayor riesgo de delito. La eficiencia operativa se ha mejorado, pero la política también ha sido tachada de sinónimo de enfocar la vigilancia en varios barrios, reafirmando estigmas preexistentes.

Consistente con la premisa de la Teoría del Control Social (Hirschi, 1969) de que los vínculos sociales fuertes disminuyen la probabilidad de delincuencia, la IA se ha aprovechado para rastrear factores de riesgo en comunidades de alto riesgo y movilizar acciones preventivas tempranas. Actividades como programas educativos de IA del Reino Unido orientados a relaciones comunitarias más sólidas, así como a detener a los jóvenes de seguir caminos delictivos, también están generando preocupaciones sobre la privacidad y el potencial para la aplicación automática de datos sensibles, especialmente para los jóvenes.

Según la Teoría del Aprendizaje Social (Bandura, 1977), el comportamiento humano se aprende mediante la observación y la imitación de otros. En ese sentido, la IA ha sido utilizada para identificar patrones delictivos en un escenario digital, por ejemplo, el ciberacoso o la radicalización en línea. Los algoritmos que trabajan en plataformas como Facebook o Twitter pueden resultar en evaluaciones de amenazas en tiempo real. Sin embargo, esos sistemas no están libres de preocupación, en su caso, la amenaza de errores, censura o vigilancia.

La Teoría de la Oportunidad (Clarke, 1980) afirma que cuando se reduce la oportunidad, se reduce la ocurrencia del delito. Por lo tanto, el reconocimiento facial y la vigilancia inteligente en video se emplean en la prevención del crimen y mejoran la capacidad de respuesta de la aplicación de la ley. China ha sido un modelo al hacer esto. Pero estas nuevas tecnologías "atractivas" tienen implicaciones legales y éticas problemáticas, incluyendo la pérdida de privacidad y el potencial de discriminación algorítmica.

La Perspectiva Funcionalista, por otro lado, desarrollada por Émile Durkheim, sostiene que el crimen resulta de una disyunción entre las metas sociales y los medios legítimos disponibles para alcanzarlas, como la falta de empleo o la falta de igualdad. Desde esta perspectiva, la IA se utiliza para analizar datos sociales masivos y sus relaciones con los indicadores delictivos. Eso podría generar políticas públicas mejor fundamentadas, pero también podría reducir un fenómeno humano complejo a una serie de variables cuantificables y expectativas poco realistas, sin mencionar antisociales, sin tener en cuenta su compleja causa social.

Esta perspectiva metodológica permite captar no solo las disponibilidades técnicas de las tecnologías de IA, sino también sus limitaciones morales y humanísticas. La Tabla 1 proporciona un resumen de estas relaciones que involucran teoría criminológica, intervenciones tecnológicas y sus efectos resultantes.

Tabla 1. Relación entre teorías criminológicas y aplicaciones de la inteligencia artificial en la prevención del delito

Teoría criminológica	Autor/es	Aplicación de la IA	Ejemplos concretos	Beneficios identificados	Riesgos y Críticas
Actividades Rutinarias	Cohen y Felson (1979)	La IA como "guardián capaz": mediante sistemas de vigilancia predictiva y focalizada	Implementación de PredPol en Los Ángeles	Mejora en la asignación de recursos policiales y reducción de ciertos delitos	Estigmatización de zonas vulnerables, posible sesgo en la vigilancia focalizada
Control Social	Hirschi (1969)	Análisis de factores de riesgo en comunidades vulnerables para intervención temprana	Programas educativos basados en IA en el Reino Unido	Refuerzo de vínculos sociales y prevención del delito desde etapas iniciales	Uso potencialmente invasivo de datos sensibles; automatización de decisiones sobre menores
Aprendizaje Social	Bandura (1977)	Aplicación de IA para detectar y analizar conductas	Sistemas de detección de ciberacoso y extremismo en redes	Identificación precoz de conductas violentas; prevención	Riesgo de falsos positivos, censura de contenidos, vigilancia

		delictivas en entornos virtuales	como Facebook o Twitter	de radicalización digital	indiscriminada
Oportunidad	Clarke (1980)	Reducción de oportunidades delictivas mediante tecnologías de reconocimiento facial y videovigilancia	Cámaras inteligentes con IA en espacios públicos en China	Disuasión efectiva del delito, mayor capacidad de respuesta de las autoridades	Posibles abusos en el uso de datos biométricos; discriminación algorítmica; pérdida de privacidad
Funcionalismo	Émile Durkheim (1893-1897)	Uso de IA para análisis estructural del delito, conectando variables sociales con patrones criminales	Análisis de correlaciones entre desempleo, pobreza o desigualdad y delitos	Mejor comprensión del delito como fenómeno social; base para políticas públicas efectivas	Reducción del enfoque criminológico a simples correlaciones; posible deshumanización del análisis

Fuente: Elaboración propia a partir de Cohen y Felson (1979), Hirschi (1969), Bandura (1977), Clarke (1980) y Durkheim (1893–1897).

3. METODOLOGÍA

3.1 Revisión de la literatura

Dada la complejidad de un problema tan multidimensional como el uso de la inteligencia artificial en el ámbito del castigo, fue necesario contar con una base documental adecuada y heterogénea. El objetivo no era simplemente recopilar datos, sino iluminar las muchas dimensiones sociales, legales, técnicas y éticas que atraviesan este software.

También nos referimos a teorías criminológicas como las Actividades Rutinarias, el Control Social, el Aprendizaje Social, la Oportunidad y el Funcionalismo durante la revisión de artículos académicos. Por esta razón, también se consideraron artículos académicos recientes que ofrecían nuevos enfoques teóricos y metodológicos, así como informes elaborados por agencias internacionales como Europol, cuya experiencia operativa es indispensable para comprender cómo se están utilizando estas herramientas en la práctica.

Además se utilizaron publicaciones especializadas relacionadas con la tecnología, la seguridad y la justicia digital para mejorar la cobertura. Esta mezcla de fuentes proporcionó un contrapeso entre el "lenguaje académico" y lo que las instituciones y operaciones tratan.Desde el principio, se pretendía que fuera más que meramente técnico y más bien una manera de vincular los desarrollos tecnológicos con sus efectos reales sobre los seres humanos y el aparato del castigo.

Para asegurarse de que la información analizada fuera actual y de alta calidad, se establecieron criterios de selección, favoreciendo textos escritos en los últimos 5 años, preferiblemente con estudios de caso, análisis críticos y encuestas de impacto. También se apreciaba la relevancia de los contenidos en relación con el escenario europeo, ya que el contexto nacional es un mapeo necesario para entender las políticas públicas y la regulación sobre el uso de la IA para la seguridad.En cambio, se rechazaron fuentes que prometían un tratamiento superficial, conjetural o no basado en evidencias. Esta elección controlada de las fuentes de citas permitió establecer un marco teórico con coherencia entre los objetivos de este trabajo y la realidad de los mismos en cuestión.

3.2 Consideraciones éticas

Los análisis presentados aquí se han realizado únicamente sobre fuentes de datos secundarias, por lo que la necesidad de una aprobación ética formal específica no es aplicable. No obstante, se han aplicado criterios de rigor ético a lo largo de todo el proceso de análisis, especialmente en el tratamiento de casos delicados o reales. En este sentido, se llevaron a cabo intentos para evitar cualquier revictimización, asegurando la dignidad de las personas afectadas, incluso cuando la información era de conocimiento público. Asimismo, se ha limitado cualquier forma sensacionalista de abordar esto, para dar paso a una interpretación científica, imparcial y profesional de los eventos.

3.3 Análisis de casos

En este trabajo, con el fin de comprender la aplicación de la inteligencia artificial en el campo de la seguridad, se analizan cuatro experiencias: tres intervenciones policiales de alto impacto internacional y una herramienta institucional de uso constante. Aunque sus métodos puedan diferir, todos tienen un denominador común subyacente: la utilización de tecnología de vanguardia para prevenir o adelantarse a operaciones delictivas sofisticadas.

La elección de estos casos se guía por los siguientes criterios: incluir una diversidad de métodos empleados, fiabilidad de la información, relación directa con el ámbito europeo y capacidad para ilustrar tanto los logros como las controversias asociadas al uso de estas herramientas. Cada uno abre la discusión sobre aplicaciones específicas, desde la operación aplicada contra las redes criminales hasta los sistemas predictivos para la gestión de riesgos urbanos.

Más allá de los aspectos técnicos, la selección de estos casos responde a una necesidad fundamental: saber cómo estas tecnologías tienen un impacto en las decisiones que, en última instancia, afectan a las personas comunes. En escenarios donde las conversaciones privadas son espiadas, la vigilancia opera automáticamente o ciudades enteras son sometidas a actos, uno debe preguntarse no si la herramienta funciona, sino cómo reconfigura la relación entre ciudadano, tecnología y justicia. ¿Qué hace con la vida cotidiana, la confianza en las instituciones o los derechos de aquellos que podrían atraparse inadvertidamente?

No se trata sólo de describir qué tecnologías se utilizaron y con qué éxito. El atractivo radica en ver el conjunto, los objetivos que se proponen, las decisiones que enfrentan, los dilemas morales que se desarrollan y los daños sociales que causan. Esta comprensión holística permite responder al fenómeno con mayor sensibilidad, abordando no sólo la eficiencia operativa de la decisión, sino también sus dimensiones legales, políticas y humanas.Cada uno de los casos aquí detallados se desarrolla completamente en el capítulo 4 y se abordan las contribuciones, los desafíos detectados y las reflexiones que permiten indagar sobre la presencia de la inteligencia artificial en la construcción de la seguridad pública hoy en día.

3.4 Muestra de población diana

Este estudio no se fundamenta en una muestra numérica ni en una población estadística tradicional, sino en el estudio de casos específicos que, debido a su importancia y unicidad, facilitan la comprensión del uso de la inteligencia artificial en el campo de la seguridad. En vez de enfocarse en individuos, la atención se dirige a dos grandes protagonistas: por un lado, las organizaciones delictivas que han utilizado tecnologías de vanguardia para realizar sus acciones; por otro, las instituciones que han creado herramientas basadas en Inteligencia Artificial para enfrentarlas.

Los ejemplos seleccionados facilitan la observación del fenómeno desde ambos extremos del conflicto: aquellos que emplean la tecnología como instrumento para esconderse, comunicarse o ampliar su actividad, y aquellos que la emplean como herramienta para prever peligros, interceptar redes y responder con mayor poder. Esta doble visión guía el análisis y proporciona una imagen más justa de cómo opera la inteligencia artificial en un entorno tan complicado como el mundo real. La dimensión europea se ha fortalecido no solo por la disponibilidad de datos y la importancia de operaciones específicas, sino también porque Europa tiene un papel líder como referente en la regulación de estas tecnologías. El análisis de casos ocurridos en este contexto geográfico facilita la conexión directa entre las acciones de campo y las regulaciones destinadas a restringir sus excesos y asegurar el cumplimiento de los derechos básicos.

En definitiva, la selección de estas experiencias no solo se basa en su efecto operativo, sino también en su capacidad para generar interrogantes fundamentales: ¿cuánto puede avanzar la tecnología en pos de la seguridad? ¿Qué protecciones son imprescindibles para prevenir elecciones injustas o automatizadas sin supervisión humana? Estos son los factores que respaldan la selección de la muestra y guían el enfoque crítico de este estudio.

3.5 Diseño de investigación

Este es un estudio cualitativo-descriptivo realizado a través análisis bibliográfico y de casos relevantes. El objetivo es comprender el uso de la IA en la criminología contemporánea, especialmente para identificar y mitigar actividades delictivas.

El enfoque integra una revisión de literatura de libros especializados con el análisis de experiencias del mundo real, caracterizado por la aplicación de estas tecnologías. Con este fin, se han seleccionado tres operaciones internacionales: EncroChat, Matrix, Operación Ghost, que han aplicado diferentes niveles de IA en la lucha contra la delincuencia organizada. La evaluación del Sistema de Anticipación del Crimen (CAS) también se incorpora como un ejemplo de un aparato predictivo institucionalmente continuo.

Este documento compara las diferentes maneras en que se está utilizando la IA, y al hacerlo es capaz de resaltar algunas de las similitudes, diferencias significativas y temas recurrentes entre ellas. De este modo, al mismo tiempo, proporciona un enfoque en aspectos con frecuencia decisivos, como cómo se alinean varias instituciones, las directivas sobre cómo se usan, y también las cuestiones éticas que surgen con el desarrollo de estas tecnologías.

El estudio se organizó en los siguientes tres pasos. Primero, se recopilaron e identificaron datos en fuentes especializadas. Finalmente, se examinaron los resultados de discriminación para casos especiales seleccionados. Resumen útil: una discusión de los resultados desde una perspectiva analítica se llevará a cabo, con el fin de crear una visión que pueda conducir a mejorar lo que ya se está haciendo y aplicar el resultado en el futuro.Con tal enfoque, ordenadamente vemos el tema en cuestión, facilitando así la comprensión tanto de las potencialidades que la Inteligencia Artificial ofrece para la seguridad como de los conflictos o dudas que surgen en su implementación.

4. RESULTADOS

4.1 Síntesis de los casos analizados

El análisis de los casos seleccionados permite ver cómo la inteligencia artificial está transformando las formas en que se enfrentan los delitos, especialmente en lo relacionado con la prevención, el manejo de grandes volúmenes de información y la identificación de patrones delictivos. Las experiencias recopiladas muestran diferentes formas de aplicar esta tecnología: algunas enfocadas en herramientas de uso institucional y otras en operaciones específicas a gran escala.

Para ofrecer una visión más clara de estas iniciativas, se ha elaborado una tabla comparativa que resume los elementos más destacados de cada caso. En ella se recogen las tecnologías empleadas, los principales objetivos de su uso, los resultados alcanzados y los

desafíos que surgieron durante su implementación. Se incluyen, por ejemplo, operaciones como EncroChat, que logró intervenir comunicaciones cifradas y obtener miles de arrestos, o Matrix, centrada en la detección de redes criminales mediante patrones criptográficos. También se analiza la Operación Ghost, orientada a combatir el crimen organizado transnacional con herramientas de análisis forense digital.

Cada uno de estos ejemplos proporcionan importantes enseñanzas acerca del rol que puede tener la inteligencia artificial en el sector de la seguridad, pero también resalta los riesgos y retos propios de su implementación. Elementos como la salvaguarda de la privacidad, el acatamiento de las garantías procesales y la colaboración legal eficaz entre los Estados son fundamentales y no pueden ser desestimados.

Estas experiencias evidencian que, a pesar de que la Inteligencia Artificial posee un enorme potencial, su eficacia se ve afectada por diversos factores: el marco regulatorio en el que se aplica, la cooperación entre entidades, la claridad en la operación de los sistemas y, principalmente, la observancia de los derechos esenciales. Es esencial analizar meticulosamente estos componentes para comprender el auténtico rango de su influencia en las políticas de seguridad pública.

A continuación, se presenta una tabla comparativa que resume los aspectos más relevantes de los casos analizados:

Tabla 2. Comparativa de operaciones internacionales con aplicación de inteligencia artificial

Caso	Tecnología de IA implementadas	Uso principal	Resultados alcanzados	Desafíos señalados
EncroChat	Procesamiento de lenguaje natural (PLN), análisis de	Intervención y análisis de comunicaciones encriptadas	Más de 6.500 personas detenidas e incautaciones valoradas en aproximadamente 900	Controversias sobre la privacidad y el marco legal de las interceptaciones

	datos cifrados		millones de euros	
Matrix	Machine learning, análisis de patrones criptográficos	Neutralización de redes criminales complejas	Intercepción de 2,3 millones de mensajes y numerosas detenciones	Coordinación jurídica internacional y trazabilidad de la evidencia digital
Operación Ghost	Inteligencia artificial forense, análisis de redes de comunicación	Combate al crimen organizado de carácter transnacional	51 arrestos y decomisos de armas, sustancias ilegales y dispositivos cifrados	Protección de derechos procesales y retos en la vigilancia más allá de fronteras

***Fuente**: Elaboración propia a partir de Europol (2020–2024) y Eurojust. Comunicados oficiales y documentación operativa.*

4.1.2 Identificación de desafíos éticos y técnicos

Éticamente, uno de los mayores problemas del uso de la IA en la prevención del delito es la posibilidad de discriminación algorítmica. Sabiendo que tales sistemas se entrenan con enormes volúmenes de datos históricos es posible que los sistemas de IA pueden reforzar los sesgos del pasado, tratando desigualmente a ciertos grupos sociales. Esto, a su vez, plantea preocupaciones sobre la equidad en la aplicación de la ley y la necesidad de crear modelos más transparentes y auditables.

Estas tecnologías tienen el potencial de violar derechos básicos como la privacidad y la protección de datos personales. La vigilancia masiva y el análisis de grandes datos por los servicios de seguridad y la policía requieren un marco sólido de regulación, si queremos mantener este equilibrio entre prevenir el crimen por un lado y proteger los derechos civiles por el otro.

Las comunicaciones digitales se están volviendo cada vez más sofisticadas en lo que es una lucha muy dura; los criminales usan sistemas de encriptación de alto nivel y técnicas de ocultamiento digital para asegurarse de que las fuerzas del orden no puedan acceder a la

información que necesitan. Esto impulsa a la comunidad científica de ciberseguridad y forense digital a esforzarse por una capacidad mejorada para descifrar mensajes encriptados y analizar comportamientos criminales en el mundo digital. Además, dado que las tácticas criminales siguen evolucionando, las técnicas de IA deben seguir siendo adaptables a las amenazas actuales para evitar que se vuelvan obsoletas mucho antes de lo esperado.

4.2 Implicaciones para la criminología y la seguridad pública

Los casos analizados y las aplicaciones actuales de inteligencia artificial evidencian un cambio de paradigma en la manera en que se concibe, analiza y enfrenta la criminalidad. La irrupción de estas tecnologías ha ampliado las capacidades del sistema penal, pero también ha generado tensiones importantes que invitan a repensar algunos fundamentos de la criminología contemporánea. Sin embargo, en el caso de España, aún no se ha implementado plenamente la inteligencia artificial en las fuerzas policiales, lo que contrasta con los avances observados en operaciones internacionales como EncroChat, Matrix u Operación Ghost.

Desde una perspectiva operativa, la IA ha mejorado los mecanismos de prevención, análisis y respuesta ante el delito, lo que supone una transformación en los modelos tradicionales de vigilancia e investigación. La posibilidad de anticipar patrones delictivos o analizar en tiempo real grandes volúmenes de datos redefine el rol de las instituciones de seguridad, haciéndolas más reactivas, pero también más dependientes de la infraestructura tecnológica.

Ahora bien, desde una perspectiva jurídica, el despliegue de tecnologías basadas en inteligencia artificial en el ámbito de la criminología y la seguridad pública requiere someterse a límites normativos claramente establecidos. En este sentido, el Artículo 5 del Reglamento Europeo de Inteligencia Artificial (AI Act) identifica un conjunto de prácticas expresamente prohibidas por ser incompatibles con los valores fundamentales de la Unión Europea. Se prohíbe, por ejemplo, el uso de sistemas que manipulan el comportamiento humano mediante técnicas subliminales, que exploten vulnerabilidades relacionadas con la edad, discapacidad o situación económica, o que evalúen el riesgo delictivo de una persona basándose exclusivamente en perfiles o características personales, sin hechos verificables (Ley de Inteligencia Artificial, 2025). Estas disposiciones reflejan la necesidad de proteger la dignidad, la autonomía y los derechos fundamentales frente a aplicaciones tecnológicas que podrían derivar en decisiones automatizadas discriminatorias o injustificadas.

Complementariamente, el Artículo 27 del mismo reglamento establece la obligatoriedad de realizar una evaluación del impacto sobre los derechos fundamentales antes de utilizar sistemas de alto riesgo, su entrada en vigor es el 2 de febrero de 2026, esta evaluación, que debe considerar las personas o colectivos afectados y las posibles consecuencias jurídicas, representa una herramienta esencial para garantizar la proporcionalidad y la legalidad del uso de IA en contextos sensibles como la justicia penal.

En el marco legal español se regula mediante los artículos 1, 4 y 10 de la Agencia Española de Supervisión de la Inteligencia Artificial (AESIA). Esta Agencia fue aprobada por el Real Decreto 729/2023 mediante el artículo único de sus disposiciones, tomando en cuenta la facilitación de la cooperación internacional en materia de inteligencia artificial del Ministerio de Defensa en su disposición adicional cuarta. Funciones clave como la supervisión, sanción, asesoramiento y formación en el uso ético y legal de la IA también son recogidas en el Estatuto de Real Decreto 729/2023. Es por este contexto jurídico que la AESIA es garante institucional del cumplimiento normativo en el uso de la IA, promoviendo un desarrollo tecnológico responsable y transparente, respetando los principios democráticos y los derechos fundamentales.

4.2.1 Relación con Objetivos de Desarrollo Sostenible propuestos por la PNUD

La introducción de la inteligencia artificial (IA) en la criminología no solo interrumpe las formas establecidas de investigar el crimen, sino que también cuestiona las premisas subyacentes en las elecciones sobre las cuales construimos nuestra tecnología. En este sentido, tiene sentido vincular este fenómeno a varios Objetivos de Desarrollo Sostenible (ODS) definidos por el Programa de las Naciones Unidas para el Desarrollo (PNUD), en particular al ODS 9 (Industria, Innovación e Infraestructura), ODS 12 (Producción y Consumo Responsables) y ODS 10 (Reducción de las Desigualdades).

El ODS 9 enfatiza la importancia de la infraestructura inclusiva y sostenible, la innovación y el acceso ubicuo a las tecnologías de la información y la comunicación. Desde este punto de vista, el uso de la IA para la seguridad pública debería ser una estrategia de implementación, una que busque no solo la eficiencia operativa, sino también la inclusión digital, la transparencia y el acceso igualitario.

Dado que alrededor de la mitad de la población mundial (más de 4 mil millones de personas) todavía no tiene conectividad a Internet, la introducción de sistemas algorítmicos en la toma de decisiones públicas debe hacerse con prudencia, porque en ausencia de políticas de democratización de la tecnología, esta medida puede exacerbar en lugar de mejorar las desigualdades existentes (Programa de Naciones Unidas para el Desarrollo, 2015).

Casos como EncroChat, Matrix o la recientemente anunciada Operación Ghost, son una demostración vívida de cómo un ecosistema digital bien establecido puede tener un impacto significativo en la lucha contra delitos graves, en la coordinación entre entidades internacionales, agencias y su nivel de protección para los ciudadanos. Pero también subrayan una verdad básica: no todos los países están igualmente equipados para responder eficazmente. La implementación de tecnologías de última generación dirigidas a la lucha contra el crimen depende en gran medida de la disponibilidad de una infraestructura de red segura, de equipos de extracción específicos y de la legislación desarrollada al nivel más reciente.

Incorporando esta perspectiva en la investigación criminológica, podemos comenzar a ir más allá de la efectividad sobre el papel. Nos desafía a pensar sobre cómo y por qué usamos la tecnología y quién se beneficia realmente. La infraestructura no es solo la materia de la que está hecha la vida, sino también las condiciones de acceso, justicia y responsabilidad social. Desde esta perspectiva, el ODS 10 es crucial. Este objetivo subraya la necesidad de corregir las desigualdades estructurales, ya sea entre países o dentro de ellos. Bajo una lente de seguridad pública, el despliegue de tecnologías basadas en IA puede tener un impacto dispar si no está acompañado de políticas de equidad y participación ciudadana.

Donde estos instrumentos no se practican de manera uniforme, o no toman en cuenta los contrastes sociales y económicos en las comunidades, pueden promover desigualdades reforzantes. Además, la falta de directrices y sistemas de autocontrol podría resultar en soluciones automatizadas que afectan más duramente a las poblaciones desfavorecidas con muy pocos medios de apelación o revisión.

El ODS 12 recuerda que el desarrollo no puede seguir la lógica del consumo infinito, incluso en tecnología. Aunque generalmente pensamos en este objetivo en términos de por qué es importante gestionar el medio ambiente o los recursos naturales, también nos lleva a considerar los tipos de sistemas que desarrollamos y usamos, qué constituye la justicia y hasta qué punto estos sistemas son indispensables.

Casos como EncroChat o Operación Ghost muestran que el uso de la tecnología puede ser potente, pero también selectivo y bien fundamentado. No se trataba de herramientas de vigilancia masiva, sino de estrategias específicas con un objetivo claro, fundamentadas en sólidas investigaciones y con coordinación internacional. Por el lado negativo, los datos pueden recopilarse sin control, pueden comprarse sistemas costosos por capricho y no ser evaluados, la tecnología puede usarse simplemente por una tendencia, sin considerar las implicaciones éticas o sociales. Eso también es una forma de desperdicio.

El consumo responsable no significa necesariamente comprar menos o reciclar; es utilizar la tecnología con sentido común, solo cuando sea necesario, pensando siempre en cuáles son las consecuencias a medio y largo plazo. La seguridad no requiere más tecnología, sino mejores criterios. Esto es lo que significa usar el ODS 12 como un marco de referencia en este ámbito: un compromiso con la eficiencia, la ética y la sostenibilidad, en lugar de descubrir un uso para la tecnología por el simple hecho de usarla.

Tabla 3. Reflexión ética en relación con los Objetivos de Desarrollo Sostenible

ODS	**Cuestión ética principal**	**Relación con el trabajo**	**Comentario crítico**	**Propuesta**
ODS 9 *Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación*	Desigualdad en el acceso a tecnología y capacidades institucionales para utilizar IA	Las operaciones EncroChat y Ghost muestran cómo una infraestructura avanzada facilita la acción contra el crimen organizado	La innovación debe ir acompañada de medidas que garanticen el acceso equitativo a herramientas digitales, evitando que solo ciertos países puedan aplicar IA con eficacia (PNUD, 2015).	Impulsar políticas de cooperación internacional que favorezcan la equidad tecnológica en la lucha contra el crimen.
ODS 10 *Reducir la desigualdad en y entre los*	Posible reproducción de desigualdades sociales a través de	El uso de IA en seguridad puede tener efectos desiguales	Resulta fundamental asegurar que estos sistemas no perpetúen estigmas ni aumenten la vigilancia sobre	Establecer auditorías independientes y garantizar la transparencia algorítmica, con énfasis en la

países	algoritmos o uso selectivo de vigilancia	si se aplica sin perspectiva crítica ni controles adecuados.	colectivos vulnerables sin una justificación objetiva.	protección de los derechos fundamentales.
ODS 12 *Garantizar modalidades de consumo y producción sostenibles*	Uso excesivo o no justificado de recursos tecnológicos en la seguridad pública	Algunas tecnologías aplicadas en contextos reales han demostrado su utilidad cuando se usan de forma focalizada y con base empírica.	La adopción tecnológica debe estar guiada por criterios de necesidad y eficacia, evitando su implementación por inercia o sin evaluación de impacto social (PNUD, 2015).	Aplicar criterios de pertinencia y sostenibilidad antes de incorporar tecnologías; priorizar utilidad, necesidad y respeto por la privacidad.

Fuente: *Elaboración propia a partir del Programa de las Naciones Unidas para el Desarrollo (PNUD, 2015).*

4.3 Impacto en la colaboración internacional

La inteligencia artificial está reescribiendo el libro sobre cómo los países combaten y trabajan con las organizaciones de seguridad de otras naciones, cómo se comparte la información y cómo se llevan a cabo las operaciones multinacionales. Su capacidad para procesar y reaccionar rápidamente a los datos ha sido vital en la lucha contra el crimen organizado, permitiendo una respuesta más ágil y efectiva a las amenazas globales (Brantingham, 2020).

Optimizar los sistemas de vigilancia y los sistemas de alerta temprana es una de las ventajas clave de la IA en este ámbito. También parece que el éxito en identificar, investigar y desmantelar delincuentes a nivel internacional se ve complementado por bases de datos más sofisticadas y conectadas, así como por software de análisis de patrones de crimen. Esta facultad ha sido crucial en los casos antes mencionados, ya que gracias a la inteligencia artificial se logró el desmantelamiento de organizaciones criminales que operan transnacionalmente (Europol, 2022).

Además, la automatización de la recopilación y análisis de datos ha mejorado enormemente la capacidad para detectar comportamientos problemáticos rápidamente. Las fuerzas de seguridad tienen una mayor capacidad para intercambiar datos y coordinar operaciones conjuntas con mayor precisión. Esto se ha vuelto especialmente crucial en la lucha contra la trata de personas, el narcotráfico y el terrorismo, ya que la cooperación a través de jurisdicciones es fundamental para apoyar investigaciones exitosas (UNODC, 2021). Pero integrar la IA en la cooperación mundial también presenta desafíos. La interoperabilidad de los sistemas, la alineación legal y la protección de la privacidad son factores que deben armonizarse para un uso apropiado y ético de estas tecnologías.

5. DISCUSIÓN

5.1 Comparación con estudios previos

La evidencia de la investigación está en concordancia con trabajos que han identificado a la inteligencia artificial como capaz de reconfigurar políticas de seguridad. A diferencia de estudios previos que se concentraron en modelos teóricos y soluciones técnicas específicas, en lugar de tener un enfoque teórico sobre el tema, en este estudio se muestra una perspectiva desde la práctica operativa, tomando en cuenta eventos recientes que pueden proporcionar una base sólida para concluir las ventajas y desventajas de tales nuevas tecnologías.

A diferencia de un enfoque general en herramientas de software predictivo o en el desarrollo aislado de la capacidad técnica este estudio considera cómo se ha empleado la inteligencia artificial en la práctica en las líneas del frente en la lucha contra el crimen organizado. De este modo, se suma a la discusión no solo aportando evidencia sobre cuán efectiva podría ser tal medida, sino también sobre cuáles podrían ser las implicaciones legales, éticas y sociales.

Este estudio se caracteriza por su enfoque en la interrelación entre tecnología, regulación y cooperación internacional; una dimensión que tiende a pasarse por alto o subestimarse en otros estudios. Tomemos cualquiera de estos casos ya sea EncroChat, Matrix o Ghost y es claro que la IA no funciona dentro de una burbuja técnica, sino en escenarios institucionales donde las decisiones judiciales, los acuerdos transfronterizos y los márgenes interpretativos legales se encuentran.

El argumento es que una perspectiva excesivamente tecnocéntrico ha caracterizado la literatura académica hasta la fecha, y se ofrece una visión alternativa en respuesta a esto. Si bien abundan las evidencias sobre la efectividad de la inteligencia artificial en predecir delitos o asignar mejor los recursos, las implicaciones a largo plazo de esto aún se encuentran algo inexploradas. Algunas de estas pueden ser la automatización de desigualdades existentes, la falta de transparencia en cómo funcionan ciertos sistemas o la posible cesión del juicio humano en decisiones penales críticas.

Finalmente, este estudio refuerza la necesidad de enfoques interdisciplinarios, proponiendo que la inteligencia artificial no puede reducirse a un recurso neutral, y reaviva el debate sobre el uso securitizado de la inteligencia artificial desde la perspectiva de la criminología crítica, enfocándose no solo en su capacidad técnica, sino también en términos de su influencia en la justicia social, la gobernanza y los derechos fundamentales.

5.2 Limitaciones del estudio

El presente estudio actúa como una continuación de estudios previos y representa una perspectiva renovada sobre el efecto de la inteligencia artificial en la criminología y la seguridad pública. Sin embargo, es importante señalar ciertas limitaciones de la metodología utilizada. En primer lugar, el secreto de ciertas operaciones ha limitado la oportunidad de obtener información detallada sobre procesos técnicos y deliberaciones judiciales respecto a algunos componentes operativos.

La investigación se ha limitado a ejemplos europeos, lo que afecta la extrapolación de los resultados a entornos de diferentes países con diferentes requisitos regulatorios, infraestructuras y necesidades de seguridad. Por tanto, puede ser necesario realizar investigaciones comparativas en otras partes del mundo. Debido a que la inteligencia artificial avanza a un ritmo tan rápido, los resultados sobre los métodos cubiertos aquí pueden quedar fácilmente superados por otras tecnologías o metodologías. Esta variabilidad exige que actualicemos continuamente nuestro repertorio analítico y reevaluemos cómo se relaciona con el discurso de seguridad y la protección de los derechos fundamentales.

5.3 Futuras líneas de investigación

Para desarrollar la comprensión de lo que significa aplicar la inteligencia artificial en criminología y de la relación entre las fuerzas del orden y los ciudadanos, debemos explorar nuevas vías de investigación que estén orientadas hacia la práctica, la ética y las implicaciones sociales de adoptar la IA. Un área de enfoque es la comparación internacional de modelos de implementación. Una comparación de la implementación de la IA en seguridad entre países también permitiría medir ciertos indicadores: la posición de la ley, la transparencia, la participación ciudadana, la concentración tecnológica o similares. Esto nos permitiría aprender de las mejores prácticas y adaptar un enfoque más justo in situ.

Los efectos a largo plazo de estas tecnologías también deben ser considerados. Necesitamos aprender todo lo posible sobre algo más que solo cómo funcionan a corto plazo; necesitamos entender cómo afectan la psicología de la seguridad, la confianza en las instituciones que las implementan, y si, a largo plazo, reducen el crimen. A través de la adición de medidas sociales y cualitativas, podemos medir no solo lo que hace la IA; también podemos evaluar cómo la IA cambia las relaciones de estado, tecnología, sociedad.

Un segundo gran desafío es desarrollar planes de ética y evaluación adecuados. La regulación no puede ser simplemente un ejercicio de redacción; también debe incluir herramientas prácticas para mitigar riesgos, como el sesgo algorítmico, la censura excesiva y el despliegue opaco de herramientas de automatización. Eso significa defender una IA que no solo sea eficiente, sino también legítima y aceptada por la sociedad. Se propone una agenda que va más allá del discurso técnico y se posiciona en una comprensión más multifacética, reflexiva y crítica de la IA en criminología. Solo de esta manera podemos pensar en modelos de seguridad pública realmente sostenibles que estén basados en los derechos humanos y centrados en las personas, como debería ser.

6. CONCLUSIONES Y PROPUESTAS

6.1 Resumen de hallazgos clave

Basado en el análisis desarrollado en este trabajo, podemos afirmar que la IA no solo mejora el potencial técnico de los sistemas de seguridad, sino que también cambia profundamente la manera en que se conciben y abordan los fenómenos criminales. Su aplicación a la predicción del crimen, el análisis forense de datos complejos y la vigilancia

digital de comportamientos sospechosos ha permitido sucesivamente encontrar patrones que emergen una y otra vez, una asignación inteligente de recursos y la disminución de los tiempos de respuesta de las instituciones ante nuevas amenazas. Para la predicción del crimen, los datos históricos incluyen ubicaciones, hora del día, perfiles de actores y tipos de delito, y los algoritmos predicen lugares y momentos con mayor probabilidad de cometerse un delito. Esta estrategia permite que las medidas preventivas y la asignación de recursos sean más eficientes. Alternativamente, el análisis forense totalmente automatizado con medios como el procesamiento de lenguaje natural (PLN) puede ayudar en la interpretación de un gran conjunto de datos cifrados o no estructurados, lo cual es esencial para la investigación de ciberdelitos, fraudes o terrorismo digital.

La vigilancia digital, asistida por herramientas como el reconocimiento facial o el análisis de redes sociales, puede proporcionar esa capa adicional para detectar patrones sospechosos, relaciones entre sujetos y restos entre evidencia de actividades criminales potenciales, aumentando así los poderes de investigación, sin necesidad de que un operador siempre esté involucrado. Más allá de su relevancia práctica, la IA ofrece una reorganización del modelo de prevención y control en términos estructurales: la velocidad y automatización del procesamiento de datos coinciden con aspectos controvertidos relacionados con la legalidad y la supervisión.

El trabajo ha demostrado que los algoritmos no son neutrales: pueden introducir sesgos, cometer juicios erróneos o transferir la responsabilidad de los humanos a ellos en procesos de decisión con un contenido moral. La revisión sugiere que no se trata de tecnicismos, sino de si estas herramientas están integradas en entornos institucionales legítimos, con las salvaguardas adecuadas, y educación específica de alto estándar ético. Por esa razón, el avance de la inteligencia artificial no significa automáticamente que el sistema de justicia mejore, pero puede ser una fuerza positiva si se utiliza adecuadamente con sabiduría, transparencia y respeto a los derechos fundamentales.

El verdadero desafío no es solo tecnológico, sino también político, regulatorio y cultural: incorporar esas tecnologías sin perder de vista los valores en los que debería descansar cualquier política de seguridad pública. La investigación realizada confirma que la efectividad de esta tecnología está más relacionada con su uso en contextos institucionales reales (con suficientes controles, personal capacitado y un marco normativo sólido) que con sus capacidades técnicas.

La IA ética significa aplicar un conjunto de prácticas específicas: auditar regularmente los algoritmos para encontrar y corregir sesgos, asegurar que los sistemas sean transparentes y explicables, mantener el control humano sobre decisiones críticas y encontrar entrenadores profesionales para los operarios humanos de sistemas con IA.Estos son los requisitos para garantizar que los derechos no sean violados y que opere un sentido de legitimidad y confianza pública en el sistema.

Por lo tanto, la IA no promete mejorar el campo de la justicia penal per se, pero podría contribuir eficazmente a fortalecerlo siempre que se utilice de manera responsable, con prudencia técnica y transparencia y con pleno respeto de los derechos fundamentales.El verdadero problema no es solo tecnológico, también es político, regulatorio y cultural: incorporar estas tecnologías de una manera que evite que se utilicen de una manera que pueda traicionar los valores democráticos y sociales en los que debería basarse cualquier política de seguridad pública.Dentro del ámbito de la seguridad pública, el uso de la inteligencia artificial (IA) ha hecho posible crear herramientas que predicen crímenes, analizan delitos e investigan crímenes de manera más efectiva.

Uno de los más notables es el Sistema de Anticipación del Crimen, empleado en los Países Bajos, que utiliza datos históricos para predecir regiones más propensas a robos, permitiendo la asignación más eficiente de recursos policiales. Un ejemplo es PredPol en los Estados Unidos, que predice la probabilidad de delitos en ubicaciones específicas basándose en la información espacio-temporal. Ha hecho grandes cosas para la planificación policial, por supuesto, pero también ha sido criticado por reproducir sesgos sociales.

El reconocimiento facial es otra tecnología relacionada en la que los sospechosos son identificados en espacios públicos utilizando algoritmos de visión artificial. Sin embargo, su estabilidad es menor en ciertas poblaciones, lo cual tiene implicaciones éticas. Tratando con mensajes y comunicaciones digitales, con el PLN pueden identificar amenazas, discursos radicales, criminalidad, etc. Esto se alía al examen de redes criminales, proporcionando una nueva forma de visualizar las relaciones entre individuos u organizaciones, y la IA forense acelera el proceso de examinar pistas en línea.Estas son herramientas útiles, pero esa utilidad depende de que se encuentren en la aplicación de la ley, con supervisión humana, guías éticas y la luz, esto puede deslizarse del abuso a la discriminación.

6.2 Propuestas de políticas públicas

Dado el creciente desarrollo de tecnologías basadas en IA en el ámbito de la seguridad, la forma en que integramos, monitoreamos y gobernamos estas fuerzas tecnológicas dentro de esquemas institucionales ciertamente requerirá un replanteamiento. No se trata solo de supervisar los riesgos de su uso, sino de establecer un marco de control que ponga los derechos fundamentales en el centro de las nuevas tecnologías.

Una línea de acción importante es explorar y reforzar las estructuras regulatorias existentes y los principios que van más allá del mero cumplimiento. La legalidad debe combinarse con la legitimidad y la auditabilidad técnica, especialmente en áreas críticas como la seguridad pública. Regulaciones como la Ley de IA de la UE ofrecen un buen modelo para calificar el perfil de riesgo de un sistema de IA, y el GDPR sirve como estándar adecuado para proteger la privacidad individual. Pero ambos sistemas necesitan trabajo en cuanto a cómo se utilizan en la práctica, especialmente dado el enorme uso de datos personales en operaciones policiales y de inteligencia.

En segundo lugar, la construcción institucional necesita ser un pilar estratégico esencial. El impacto en la responsabilidad corporativa de la IA debe ir más allá de una visión estrecha centrada en las habilidades técnicas involucradas e incluir una base crítica en ética, derechos digitales y poder algorítmico. Aquellos encargados de operar tales sistemas requieren herramientas para comprender, cuestionar y gestionar el comportamiento de los algoritmos en lugar de simplemente aceptar pasivamente resultados automatizados.

El progreso en mecanismos de control híbrido también es un punto crítico, para lo cual es necesario combinar control humano con supervisión automática y control de terceros por sujetos autónomos. Dicha supervisión estructural no solo ayuda a exponer fallos y sesgos, también apoya la revisión del modelo de IA basándose en el impacto social real, en lugar de verlo meramente desde la perspectiva del rendimiento técnico.

Debemos avanzar hacia una cooperación internacional más robusta y justa, basada en tratados, normas conjuntas y patrones de integración. Las redes criminales globales son dinámicas con velocidad y tecnología, y la respuesta necesita contar con una infraestructura digital compartida que sea capaz de compartir datos, herramientas y alertas de manera eficiente y humana a través de fronteras. Ejemplos como los de Europol atestiguan la posibilidad de este camino, que aún necesita de una mayor difusión y coordinación a nivel global.

En última instancia, estas propuestas ven a la inteligencia artificial como algo más allá de una herramienta técnica y como un espacio que moldea prácticas, responsabilidades y valores. La inteligencia artificial debe estar integrada en el sistema de seguridad, y los legisladores de políticas deben adoptar un enfoque colaborativo para planificar con anticipación e idear políticas destinadas a proteger a las personas en un mundo digital complejo.

6.3 Código ético sugerido para el uso de IA en la prevención del delito

La aplicación de la IA en criminología no solo debe servir para satisfacer estándares legales, sino que debe estar sujeta a reglas éticas transparentes y estrictas que gobiernan no solo su diseño, sino también su uso práctico y monitoreo regular. En un campo de consecuencias tan críticas como la seguridad pública, donde una decisión automatizada podría significar la diferencia entre la vida y la libertad de una persona, cualquier dimensión ética no es un mero complemento, es un requisito.

Tener un código de ética funcional implica transformar valores como la justicia, la equidad o la dignidad humana en normas más específicas que guíen lo que los seres humanos deben hacer en una situación dada. Los sistemas no solo deben funcionar, sino que deben funcionar con equidad y ser comprensibles y respetuosos de los derechos humanos.

Entre los estandartes de este código debería haber una doctrina: la transparencia algorítmica. Caja negra: los sistemas de recomendaciones y predicciones no deberían operar en modo de caja negra. Deben ser inteligibles, auditables y explicables no solo por los diseñadores, sino también por las personas que los implementan y las personas sujetas a sus decisiones.

El caso del algoritmo COMPAS en los Estados Unidos es una ilustración perturbadora: se usó para medir el riesgo de reincidencia en procedimientos judiciales, pero producía puntajes sin que los ciudadanos pudieran entender la base de esos puntajes. Esto resultó en juicios judiciales llevados a cabo a través de procedimientos oscuros y, a menudo, injustos (Angwin, Larson, Mattu & Kirchner, 2016).

El segundo elemento es la equidad algorítmica: los modelos deben ser entrenados, evaluados y ajustados para no reforzar las desigualdades sociales existentes. Múltiples estudios han demostrado cómo los sistemas de reconocimiento facial funcionan mal cuando se usan en

mujeres y personas de color, con efectos potencialmente devastadores como identificación errónea, arrestos falsos o incluso discriminación automática. Estas disparidades no son fallas técnicas, son síntomas de que los sistemas necesitan ser examinados críticamente y considerados socialmente.

En tercer lugar, el juicio humano aún debería utilizarse, ya que la IA puede ser una herramienta fantástica en la toma de decisiones, pero nunca debería reemplazar la capacidad de los profesionales para criticar. Cualquier decisión con consecuencias legales o sociales significativas debe ser firmada por un ser humano competente que pueda comprender la situación y aprobarla.

De lo contrario, se termina en situaciones como el sistema SyRI en los Países Bajos, que calculaba automáticamente un nivel de riesgo de que las personas fueran fraudulentas en lo social sin ninguna supervisión humana directa (Ferrer, 2020). No es sorprendente que este enfoque opaco y mecanicista resultara en un escrutinio excesivo de familias vulnerables, y fue declarado ilegal por los tribunales por violar derechos fundamentales.

Otro principio importante es lo que podría llamarse proporcionalidad tecnológica: el hecho de que algo pueda hacerse no significa que deba hacerse. Las herramientas de IA deben basarse en necesidades genuinas y ser proporcionales al riesgo identificado y deben estar basadas en evidencia. De modo que el despliegue de cámaras operadas por IA sin discreción en espacios públicos, por ejemplo, puede comenzar a socavar derechos como la privacidad o la presunción de inocencia si no hay una razón legítima para su uso.

Finalmente, un código ético debe ser mutable o revisable, ya que las tecnologías están cambiando constantemente, al igual que los riesgos y consecuencias que las acompañan. Los principios éticos no pueden ser estáticos; deben evolucionar con la edad, los aprendizajes y descartar lo que no sirve como debería. Solo un código vivo puede responder responsablemente a un mundo digital en continua transformación.

Para facilitar la comprensión y aplicación de estos principios, a continuación se presenta una tabla resumen con los principales elementos que debería incluir un código ético para el uso responsable de inteligencia artificial en la prevención del delito:

Tabla 4. Código ético propuesto para el uso de inteligencia artificial en seguridad pública

Principio ético	Aplicación concreta	Posibles consecuencias de su incumplimiento	Ejemplo real
Transparencia en los algoritmos	Es fundamental que los sistemas utilizados puedan ser auditados, comprendidos y explicados de forma clara.	La falta de claridad en las decisiones algorítmicas puede generar desconfianza institucional y limitar el derecho a defensa.	El sistema *COMPAS* en EE. UU. fue criticado por clasificar a acusados sin justificar sus criterios.
Equidad y no discriminacion	Evaluar regularmente el impacto de los modelos en poblaciones vulnerables y corregir sesgos detectados.	Si no se controlan los sesgos, se pueden perpetuar desigualdades estructurales y causar daños sociales profundos.	Los sistemas de reconocimiento facial han mostrado mayor margen de error en mujeres y personas racializadas.
Supervisión humana activa	Toda decisión sensible debería contar con validación humana por parte de personal cualificado.	Automatizar decisiones críticas sin contexto puede derivar en errores graves y falta de rendición de cuentas.	*SyRI* en Países Bajos fue anulado por señalar fraudes sin intervención ni control humano.
Uso proporcionado de la tecnología	Aplicar soluciones basadas en IA únicamente	Un despliegue excesivo o innecesario puede vulnerar derechos	Instalación indiscriminada de cámaras con IA en espacios públicos sin amenazas reales identificadas.

	cuando el riesgo lo justifique y con medidas proporcionadas.	fundamentales y suponer un mal uso de recursos públicos.	
Actualización ética continua	Revisar periódicamente los principios aplicados, ajustándose a los avances tecnológicos y sus efectos reales.	La falta de actualización puede dejar sin respuesta nuevos riesgos, restar legitimidad y generar vacíos normativos.	Aparición de nuevas formas de IA, como la generativa o emocional, sin evaluación ética previa

Fuente: Elaboración propia a partir de High-Level Expert Group on Artificial Intelligence (2019).

6.4 Reflexiones finales

Hacer este trabajo me ha hecho darme cuenta de que la IA no es simplemente el último avance tecnológico, ni es solo algo para ingenieros o empresas especializadas. Es un fenómeno que ya está cambiando de manera silenciosa y contundente la forma en que manejamos cosas fundamentales en nuestra sociedad, incluyendo la seguridad y la justicia. Cuando comencé esta tarea, veía la IA como algo distante pero casi no relacionado— relativamente a mi campo; después de profundizar más en el proceso, descubrí que su inmediatez es mucho más cercana y determinante de lo que había pensado.

El aspecto más importante de este recorrido no fue aprender cómo funcionaban los algoritmos, sino cómo sus decisiones podían impactar directamente a los individuos. A través de la investigación, encontré ejemplos reales donde, en nombre de la seguridad, un sistema automatizado puede designar a alguien como sospechoso sin una razón clara, o donde la mirada de una cámara de IA absorbe todo un vecindario porque “las estadísticas dicen” que hay más crimen en esas partes. ¿Qué sucede con las personas y las familias que viven allí? ¿Cómo se sienten viviendo bajo vigilancia si no son culpables de nada?

Uno de los ejemplos que más me conmovió fue el SyRI (sistema de indicación de riesgo) en los Países Bajos, que se utilizó para detectar fraudes potenciales basados en datos sociales y que finalmente llevó a impactar severamente las vidas de los más vulnerables sin justificación clara ni supervisión humana. Esto no es obra de ciencia ficción: ocurrió en Europa hace solo unos años; un tribunal detuvo tal sistema. Ese caso me hizo darme cuenta de que la IA no es neutral. Puede replicar prejuicios, penalizar la pobreza o propagar desigualdades en general, incluso si no lo hace "a propósito". Pero lo hace.

Como estudiante de criminología, creo que jugamos un papel crucial en todo esto. Simplemente no podemos permitir que tales juicios sobre la libertad, la privacidad y la vida de las personas sean decididos por una máquina, por muy eficiente que parezca. Nuestra tarea es continuar preguntando: ¿Quién se beneficia de esta tecnología? ¿A quién puede perjudicar? ¿Qué derechos están en juego? Y, finalmente, ¿quién tiene el poder?

Este proyecto también me ha hecho darme cuenta de la importancia de la educación interdisciplinaria. El ritmo de la tecnología ha superado la capacidad de los legisladores, éticos y organismos de supervisión para mantenerse al día. Estoy asumiendo el hecho de que no es suficiente saber sobre criminología en el sentido tradicional. También es tiempo de discutir sobre datos, algoritmos, regulación digital. Debemos casar el pensamiento crítico con el conocimiento técnico si no queremos ser excluidos de los debates sobre hacia dónde se dirige el futuro de nuestra profesión.

He encontrado que la necesidad de avanzar no es enteramente implementar nuevas tecnologías, sino implementar bien las tecnologías que ya tenemos, y con una visión humana. No podemos darlo por sentado, porque si no estamos en la mesa cuando estas herramientas son diseñadas, aplicadas y evaluadas, otros lo estarán y no estarán pensando en nuestros términos disposicionales. Y eso puede ser un gran problema.

Me quedo con más preguntas que respuestas, pero también con una certeza: esto no termina aquí con este trabajo. Todo lo contrario, sospecho que aquí comienza un camino que me encantaría seguir descubriendo. Espero seguir siendo un estudiante de esta área de investigación, para poder continuar sirviendo a mis responsabilidades y, con suerte, para poder contribuir en el futuro para asegurar que la IA proteja a las personas, en lugar de vigilarlas o excluirlas. Para que se convierta en un aliado de la justicia, en lugar de una amenaza silenciosa.

7. REFERENCIAS BIBLIOGRÁFICAS

Aguilar Cabrera, D. A. (2024). *La inteligencia artificial en la justicia: Protocolos para la presentación y la valoración de prueba digital obtenida mediante IA*. Revista Oficial del Poder Judicial, 16(22), 475–497. https://doi.org/10.35292/ropj.v16i22.1018

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016, 23 de mayo). *Machine bias: There's software used across the country to predict future criminals. And it's biased against blacks.* ProPublica. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Bandura, A. (1977). *Social Learning Theory*. Prentice-Hall. https://ia903002.us.archive.org/15/items/BanduraSocialLearningTheory/Bandura_SocialLearningTheory_text.pdf

Basu, S. (2020). Legal and human rights issues of AI: Gaps, challenges and vulnerabilities. *Journal of Responsible Technology*, 1, 9–18. https://doi.org/10.1016/j.jrt.2020.100005

Binns, R. (2018). *Algorithmic accountability and public reason*. Philosophy & Technology, 31(4), 543–556. https://doi.org/10.1007/s13347-017-0263-5

Clarke, R. V. (1980). Situational crime prevention: Theory and practice. *British Journal of Criminology, 20*(2), 136-147. https://academic.oup.com/bjc/article-abstract/20/2/136/517259

Cohen, L. E., y Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review, 44*(4), 588-608. https://doi.org/10.2307/2094589

Comisión Europea. (2022). *The Digital Services Act: Ensuring a Safe and Accountable Online Environment*. https://ec.europa.eu/

Cuadernos de Seguridad. (2024, Marzo). Inteligencia artificial y seguridad: Nuevos paradigmas para la prevención del delito. https://cuadernosdeseguridad.com/2024/03/inteligenciaartificial-seguridad/

Decide Soluciones. (2023). *Encicloped-IA: Tu diccionario de la Inteligencia Artificial y la Analítica Avanzada*. https://decidesoluciones.es/encicloped-ia/

El País. (2024, Diciembre). Cae Matrix, un servicio de comunicación encriptada que utilizaban la Mocro Maffia y otras organizaciones criminales. https://elpais.com/espana/2024-12-03/cae-matrix-un-servicio-de-comunicacion-encriptada-que-utilizaban-la-mocro-maffia-y-otras-organizaciones-criminales.html

European Commission. (2021). *High-risk AI systems and their requirements under the AI Act*. https://digital-strategy.ec.europa.eu/en

European Digital Rights (EDRi). (2022). *Digital Services Act: What You Need to Know*. https://edri.org

Europol. (2020). *Dismantling encrypted criminal EncroChat communications leads to over 6,500 arrests and close to EUR 900 million seized*. Europol. https://www.europol.europa.eu/media-press/newsroom/news/dismantling-encrypted-criminal-encrochat-communications-leads-to-over-6-500-arrests-and-close-to-eur-900-million-seized

Europol. (2024). *AI and policing: The benefits and challenges of artificial intelligence for law enforcement*. Publications Office of the European Union. https://www.europol.europa.eu

Ferrer, I. (2020, 12 de febrero). *Países Bajos veta un algoritmo acusado de estigmatizar a los más desfavorecidos*. El País. https://elpais.com/tecnologia/2020/02/12/actualidad/1581512850_757564.html

Financial Times. (2024, Agosto). Ghost: International police dismantle encrypted messaging platform used by criminals. https://www.ft.com/content/ce927443-fc93-4b88-adb3-2ed3cca8caa9

Garland, D. (2005). *La cultura del control: Crimen y orden social en la sociedad contemporánea* (J. de la Fuente, Trad.). Buenos Aires: Editorial Ad-Hoc. https://www.criticapenal.com.ar/wp-content/uploads/2014/09/culturadelcontrol.pdf

High-Level Expert Group on Artificial Intelligence. (2019, 8 de abril). *Ethics guidelines for trustworthy AI*. European Commission. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419

Hirschi, T. (1969). *Causes of Delinquency*. University of California Press.https://www.ucpress.edu/book/9780520301848/causes-of-delinquency

McCarthy, J. (2006). The Dartmouth conference: The birth of artificial intelligence. *AI Magazine, 27*(4), 10-15. https://doi.org/10.1609/aimag.v27i4.1904

Ministerio de Asuntos Económicos y Transformación Digital. (2022). *Agencia Española de Supervisión de la Inteligencia Artificial (AESIA): Objetivos y funciones* https://www.mineco.gob.es

Peña Torres, M., & Martabit Sagredo, M. J. (2024). *Inteligencia artificial y derechos fundamentales: impacto en los derechos de la privacidad*. Actualidad Jurídica, 50, 77–102. https://derecho.udd.cl/actualidad-juridica/files/2024/09/3-marisol-pena-torres-y-maria-jose-martabit-sagredo.pdf

Perry, W. L., McInnis, B., Price, C. C., Smith, S. C., y Hollywood, J. S. (2013). *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. RAND Corporation. https://www.rand.org/pubs/research_reports/RR233.html

Police1. (2024). *The future of policing: How AI is transforming police operations and digital evidence management*.

https://www.police1.com/police-products/intelligence-led-policing/the-future-of-policing-how-ai-is-transforming-police-operations-and-digital-evidence-management

Politie.nl. (2021). *Crime Anticipation System: Overview and application report*. https://www.politie.nl/binaries/content/assets/politie/wet-open-overheid/11-landelijke-eenheid/overige-documentos/2021/crime-anticipation-system/20210727---8456---besluit.pdf

Programa de las Naciones Unidas para el Desarrollo. (2015).ODS https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/

Revista Latam Digital. (2022). *El sesgo algorítmico y el enfoque del diseño sensible al valor*. https://revistalatam.digital/article/22tr02/

Russell, S., y Norvig, P. (2020). *Artificial Intelligence: A Modern Approach* (4ª ed.). Pearson. https://aima.cs.berkeley.edu/

Tandfonline. (2024). *Artificial intelligence in criminology: Challenges and opportunities*. https://www.tandfonline.com/doi/full/10.1080/19361610.2024.2331885

Turing, A. M. (1950). "Computing Machinery and Intelligence". *Mind*, 59(236), 433-460. https://courses.cs.umbc.edu/471/papers/turing.pdf

Unión Europea. (2016). *Reglamento General de Protección de Datos (GDPR)*. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32016R0679

Unión Europea. (2021). *Proposal for a Regulation laying down harmonised rules on Artificial Intelligence (Artificial Intelligence Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

Unión Europea. (2022). *Reglamento (UE) 2022/2065 relativo a los servicios digitales (Ley de Servicios Digitales - DSA)*. https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX:32022R2065

Wired. (2025). *La IA está reforzando al crimen organizado, advierte la Europol*. https://es.wired.com/articulos/la-ia-esta-esta-reforzando-al-crimen-organizado-advierte-la-europol

Wolters Kluwer. (2022). Cómo utiliza la AEAT la inteligencia artificial. *Wolters Kluwer*. https://www.wolterskluwer.com/es-es/expert-insights/como-utiliza-la-aeat-la-inteligencia-artificial

ANEXO. Declaración de uso de herramientas de Inteligencia Artificial

En la elaboración del presente Trabajo de Fin de Grado se ha utilizado la herramienta de inteligencia artificial Chat GPT-4 como recurso de apoyo para la mejora del estilo académico, la claridad expositiva y la organización de contenidos. A continuación, se detallan los usos específicos realizados:

Herramienta	**Función**	**Prompt o uso específico**
Chat GPT-4	Mejora de redacción	"Soy estudiante de Criminología. Reescribe este párrafo con un estilo más claro y técnico, sin cambiar el contenido: *La inteligencia artificial se ha convertido en una herramienta clave en la prevención del delito. Gracias al análisis de datos, permite anticipar comportamientos delictivos y optimizar los recursos policiales, aunque también plantea riesgos éticos y legales."*
Chat GPT-4	Revisión de estructura	"¿Está bien organizada esta introducción de TFG? ¿Falta algo importante?"
Chat GPT-4	Sinónimo y precisión terminológica	Dame sinónimos más técnicos o académicos para 'eficaz', 'riesgo' y 'seguridad pública' dentro del contexto criminológico."